NOTICE OF OFFICE OF MANAGEMENT AND BUDGET ACTION

Date 01/30/2009

Department of Commerce
National Oceanic and Atmospheric Administration
FOR CERTIFYING OFFICIAL: Barry West
FOR CLEARANCE OFFICER: Diana Hynek

In accordance with the Paperwork Reduction Act, OMB has taken action on your request received 06/25/2008

ACTION REQUESTED: Extension without change of a currently approved collection
TYPE OF REVIEW REQUESTED: Regular
ICR REFERENCE NUMBER: 200806-0648-019
AGENCY ICR TRACKING NUMBER:
TITLE: Southeast Region Bycatch Reduction Device Certification Family of Forms
LIST OF INFORMATION COLLECTIONS: See next page

OMB ACTION: Approved without change
OMB CONTROL NUMBER: 0648-0345
The agency is required to display the OMB Control Number and inform respondents of its legal significance in accordance with 5 CFR 1320.5(b).

EXPIRATION DATE: 01/31/2012 DISCONTINUE DATE:

BURDEN:	RESPONSES	HOURS	COSTS
Previous	5,290	6,899	339,000
New	2,615	70	639
Difference			
Change due to New Statute	0	0	0
Change due to Agency Discretion	-1,224	-5,096	0
Change due to Agency Adjustment	-1,451	-1,733	-338,361
Change Due to Potential Violation of the PRA	0	0	0

TERMS OF CLEARANCE:

OMB Authorizing Official: Kevin F. Neyland
Deputy Administrator,
Office Of Information And Regulatory Affairs

List of ICs			
IC Title	Form No.	Form Name	CFR Citation
Application/vessel information form and gear specification form	NA	Bycatch Reduction Device Testing Manual	
Station sheet evaluation form, species characterization form and length frequency form	NA	Bycatch Reduction Device Testing Manual	
Condition and fate form	NA	Bycatch Reduction Device Testing Manual	
Trip report/cover sheet	NA	Bycatch Reduction Device Testing Manual	
Independent BRD tests - duplication/mailing			50 CFR 622.41

PAPERWORK REDUCTION ACT SUBMISSION

Please read the instructions before completing this form. For additional forms or assistance in completing this form, contact your agency's Paperwork Clearance Officer. Send two copies of this form, the collection instrument to be reviewed, the supporting statement, and any additional documentation to: Office of Information and Regulatory Affairs, Office of Management and Budget, Docket Library, Room 10102, 725 17th Street NW, Washington, DC 20503.

1. Agency/Subagency originating request
DOC/NOAA/NMFS

2. OMB control number b. [ ] None
a. 0648 - 0345

3. Type of information collection (*check one*)
a. [ ] New Collection
b. [ ] Revision of a currently approved collection
c. [✔] Extension of a currently approved collection
d. [ ] Reinstatement, without change, of a previously approved collection for which approval has expired
e. [ ] Reinstatement, with change, of a previously approved collection for which approval has expired
f. [ ] Existing collection in use without an OMB control number
For b-f, note Item A2 of Supporting Statement instructions

4. Type of review requested (*check one*)
a. [✔] Regular submission
b. [ ] Emergency - Approval requested by / /
c. [ ] Delegated

5. Small entities
Will this information collection have a significant economic impact on a substantial number of small entities? [ ] Yes [✔] No

6. Requested expiration date
a. [✔] Three years from approval date b. [ ] Other Specify: /

7. Title
Southeast Region Bycatch Reduction Device Certification Family of Forms

8. Agency form number(s) (*if applicable*)

9. Keywords
"Fisheries," "Fishing" and "Fishing Vessels"

10. Abstract

Persons seeking to obtain certification for bycatch reduction devices to use on shrimp vessels, in the Gulf of Mexico or South Atlantic, must apply for authorization to conduct tests and submit the test results. The information is needed for National Marine Fisheries Service (NMFS) to determine if the equipment meets the standard that would allow its use in commercial fisheries.

11. Affected public (*Mark primary with "P" and all others that apply with "x"*)
a. x Individuals or households d. ___ Farms
b. P Business or other for-profit e. ___ Federal Government
c. ___ Not-for-profit institutions f. ___ State, Local or Tribal Government

12. Obligation to respond (*check one*)
a. [ ] Voluntary
b. [✔] Required to obtain or retain benefits
c. [ ] Mandatory

13. Annual recordkeeping and reporting burden

a. Number of respondents	32
b. Total annual responses	1,775
1. Percentage of these responses collected electronically	0 %
c. Total annual hours requested	57
d. Current OMB inventory	6,899
e. Difference	(6,842)
f. Explanation of difference	
1. Program change	(5,096)
2. Adjustment	(1,746)

14. Annual reporting and recordkeeping cost burden *(in thousands of dollars)*

a. Total annualized capital/startup costs	0
b. Total annual costs (O&M)	1
c. Total annualized cost requested	1
d. Current OMB inventory	339
e. Difference	(338)
f. Explanation of difference	
1. Program change	
2. Adjustment	(338)

15. Purpose of information collection (*Mark primary with "P" and all others that apply with "X"*)
a. ___ Application for benefits e. ___ Program planning or management
b. ___ Program evaluation f. x Research
c. ___ General purpose statistics g. P Regulatory or compliance
d. ___ Audit

16. Frequency of recordkeeping or reporting *(check all that apply)*
a. [✔] Recordkeeping b. [ ] Third party disclosure
c. [✔] Reporting
1. [✔] On occasion 2. [ ] Weekly 3. [ ] Monthly
4. [ ] Quarterly 5. [ ] Semi-annually 6. [ ] Annually
7. [ ] Biennially 8. [ ] Other (describe)

17. Statistical methods
Does this information collection employ statistical methods
[ ] Yes [✔] No

18. Agency Contact (person who can best answer questions regarding the content of this submission)
Name: Jason Rueter
Phone: (727) 824-5350

19. Certification for Paperwork Reduction Act Submissions

On behalf of this Federal Agency, I certify that the collection of information encompassed by this request complies with 5 CFR 1320.9

NOTE: The text of 5 CFR 1320.9, and the related provisions of 5 CFR 1320.8(b)(3), appear at the end of the instructions. *The certification is to be made with reference to those regulatory provisions as set forth in the instructions.*

The following is a summary of the topics, regarding the proposed collection of information, that the certification covers:

(a) It is necessary for the proper performance of agency functions;

(b) It avoids unnecessary duplication;

(c) It reduces burden on small entities;

(d) It used plain, coherent, and unambiguous terminology that is understandable to respondents;

(e) Its implementation will be consistent and compatible with current reporting and recordkeeping practices;

(f) It indicates the retention period for recordkeeping requirements;

(g) It informs respondents of the information called for under 5 CFR 1320.8(b)(3):

(i) Why the information is being collected;

(ii) Use of information;

(iii) Burden estimate;

(iv) Nature of response (voluntary, required for a benefit, mandatory);

(v) Nature and extent of confidentiality; and

(vi) Need to display currently valid OMB control number;

(h) It was developed by an office that has planned and allocated resources for the efficient and effective management and use of the information to be collected (see note in Item 19 of instructions);

(i) It uses effective and efficient statistical survey methodology; and

(j) It makes appropriate use of information technology.

If you are unable to certify compliance with any of the provisions, identify the item below and explain the reason in Item 18 of the Supporting Statement.

Signature of Senior Official or designee	Date

Agency Certification (signature of Assistant Administrator, Deputy Assistant Administrator, Line Office Chief Information Officer, head of MB staff for L.O.s, or of the Director of a Program or StaffOffice)	
Signature signed by Emily Menashes	Date 06/20/2008
Signature of NOAA Clearance Officer	
Signature signed by Sarah Brabson	Date 06/23/2008

SUPPORTING STATEMENT
SOUTHEAST REGION BYCATCH REDUCTION DEVICE CERTIFICATION
FAMILY OF FORMS
OMB CONTROL NO. 0648-0345

A. JUSTIFICATION

1. Explain the circumstances that make the collection of information necessary.

The legislative authority to collect data from the various sectors of the economy that harvest marine resources in the exclusive economic zone (EEZ) is the Magnuson-Stevens Fishery Conservation and Management Act of 1976 (Magnuson-Stevens Act), as amended. Amendment 9 to the Fishery Management Plan (FMP) for the Shrimp Fishery of the Gulf of Mexico and Amendment 2 to the FMP for the Shrimp Fishery of the South Atlantic require the use of certified bycatch reduction devices (BRD) in all penaeid shrimp trawls in the EEZ of both regions. Both amendments also contain a framework procedure for establishing and modifying the BRD testing protocol, for certifying BRD and their specifications. Regulations governing this collection are at 50 CFR 622.41. Amendment 6 to the South Atlantic FMP turned this testing authority over to the National Marine Fisheries Service (NMFS).

Trawling, in the Gulf of Mexico shrimp fisheries, results in large amounts of finfish being discarded dead. Impacts of bycatch and discards are: significant biological waste, biological overfishing of target and bycatch species, economic losses in finfish fisheries, modification of biological community structure, and possible unacceptable mortality of threatened, or endangered species. The Gulf of Mexico Fishery Management Council is concerned about the magnitude of bycatch of overfished species in shrimp trawls. The Gulf of Mexico Fishery Management Council prepared Amendment 9 to reduce the adverse impacts of shrimp trawls and thereby assist in the recovery of these resources.

Shrimp fishermen in the affected EEZ areas are required to use BRD that have been approved by NMFS. The development of BRD is a dynamic process. As fishermen and other people become more knowledgeable about the behavior of fish in shrimp trawls, they will develop new ideas on ways to reduce the incidental catch of different species of concern while minimizing the loss of shrimp.

In 2008, NMFS implemented new regulations revising and consolidating the BRD Testing Protocol Manuals of both regions, resulting in a single, unified procedure for the Gulf and South Atlantic. The rule specifies that a person who proposes a BRD for certification must test such BRD and submit the results to the Regional Administrator (RA) in accordance with the Bycatch Reduction Device Testing Protocol Manual, which contains the testing protocol and the specific reporting requirements for the test results. The South Atlantic protocol has the same wording as the Gulf protocol, which identifies that, certified observers would be used. The protocol lists qualifications that an observer must meet - not how they are trained and certified. The BRD testing manual contains the protocol that researchers must use to test the effectiveness of any new or modified BRD in reducing bycatch of finfish. It describes the experimental design and basic data requirements. Standardized forms for describing the tests and reporting their results are specified in the manual. Appendices to the manual contain data entry codes, illustrations of

fish measurements, statistical reporting zones, proper statistical analytical techniques, illustrations of key species, and other information concerning the proper conduct of testing, including data management instructions.

Any BRD that is eligible for NMFS certification must be shown to reduce the weight of finfish caught by at least 30 percent. To get a BRD certified, an individual would submit the results of BRD certification trials directly to NMFS. Such submissions would be evaluated by NMFS with the RA making the final decision on BRD certification pursuant to the certification criterion, testing protocol, and terms of the FMP.

The RA will advise the applicant, in writing, if a BRD is not certified. This notification will explain why the BRD was not certified and what the applicant may do to modify the BRD or the testing procedures to improve the chances of having the BRD certified in the future. If certification was denied because of insufficient information, the applicant will have 60 days from receipt of such notification to provide the additional information; afterwards, the applicant would have to reapply. If the RA subsequently certifies the BRD, the RA would announce the certification in the Federal Register, amending the list of certified BRD.

Upon certification, it is anticipated that the manufacturers of the BRD candidates may seek patents or copyrights for the designs. Proceeds from the sale of the certified BRD should more than offset any costs associated with the development of the device.

2. Explain how, by whom, how frequently, and for what purpose the information will be used. If the information collected will be disseminated to the public or used to support information that will be disseminated to the public, then explain how the collection complies with all applicable Information Quality Guidelines.

Submission of an application to test BRD in the EEZ to the RA begins the formal process that will either lead to the certification or rejection of the BRD candidate for use in the shrimp fisheries. Any person wishing to evaluate a BRD candidate must provide the RA with an application letter, explaining the basis for the test, as well as a completed Appendix A (vessel information form). If the RA approves the request, the RA will issue a letter exempting the applicant from the regulations requiring that certified BRD be installed in all nets. In addition to the Vessel Information form, the Gear Specification form will be filled out at the beginning of each test. During the test, the Station Sheet BRD Evaluation Form and Length Frequency Form will be filled out during each test trawl effort. These forms are completed by a Southeast Fisheries Science Center (SEFSC) approved observer, and later signed by the vessel captain, indicating he concurs that the data contained on the forms is an accurate representation of the text.

A summary of the information required in the Bycatch Reduction Device Testing Protocol Manual follows:

Appendix A. Application To Test A Bycatch Reduction Device. This form provides vessel information, applicant information, owner/operator information, and lease information for any applicant desiring to test a BRD.

Appendix B and C. Gear Specification Form. This form contains the detailed information on

the shrimp trawl, BRD and turtle excluder device (TED) for use in configuring the trawl and its components. Trip number, vessel, tow number, data, net position and control/experimental net provide the detailed information for identifying the specific tows in the test. Net type and measurements provide the detailed information for the size of the trawl. Leg line data provides information on the cables that connect to the doors. Twine, mesh and other gear measures provide the technical information for key parts of the trawl and associated components including the actual location of the BRD on the trawl. These data elements provide the technical information that net makers will use to construct the approved gear and NMFS will use to prepare the regulations.

Appendix D. Station Sheet BRD Evaluation Form. This form provides the key information on whether the BRD candidate will meet or exceed the required reduction in juvenile red snapper bycatch mortality and the associated loss in shrimp. For the control and test trawls, information such as the tow number, observer, date, time in, latitude in, longitude in, depth, hours towed, vessel speed, statistical zone, operational code, total nets, BRD net position, and control net position are required to describe the test procedures to ensure that the testing protocol is being followed correctly. Data from the control and test trawls such as the total weight of the catch, total shrimp weight, total weight and number of red snapper, number of red snapper greater than and less than 100 mm provide the necessary information for the determining the ability of the BRD to exclude red snapper and the associated loss in shrimp. Information such as comments provides additional data used to understand the results. The captain's signature provides the official results. This form is completed during the test.

Appendix E. Length Frequency Form. The focus of this activity is on red snapper, king mackerel and Spanish mackerel. Red snapper is overfished and the subject of a rebuilding schedule. King mackerel and Spanish mackerel are the subject of scientific investigation to determine what role the incidental catch in shrimp trawls has on the status of these important species. Data such as the trip number, vessel code, tow number, net position and control or test net provide the key organization elements for recording the data on fish lengths. The length of a fish is the most important element in determining the impact of the shrimp trawls (and, therefore, shrimp fleets) on these species. This form is completed during the test.

Appendix F. Species Characterization Form. This form is used to record the information on the species caught in the test and control trawls. Specific information on how to record the information is in appendix E. The data will be used to assess the environmental impact of the BRD on the species found in the Gulf of Mexico.

Appendix G. Condition and Fate. Information on the condition and fate of turtles observed during testing.

Appendix H. Trip Report/Cover Sheet Form. This form is placed on the top of the completed trip data forms and provides general information about the vessel, time at sea, tow time, gear, and turtle data. This form provides background information on the vessel, its owner, and codes (trip number, vessel, and tow number) for identifying the test. Data such as the date of the test, name of the observer, vessel name, vessel identification number, owner name, and owner address are used to identify the respondent and the legal entity controlling the testing practices of the vessel. This latter requirement is essential in monitoring the compliance of the testing protocol. Information such as the year built, vessel type, hull material, gross tonnage, engine horsepower,

and crew size, provide information used to calculate the ability of the vessel to catch shrimp. NMFS will print most of this information on this form, the sponsor will review and add his/her required information such as the Captain's or owner's signature. This information is completed at the start of the test.

Observer Qualifications

An observer must have a Bachelor's degree in fisheries biology or closely related field from an accredited college, have at least six months experience working with a university, college, state fisheries agency, NMFS, or private research organization such as the Gulf and South Atlantic Fisheries Foundation as an observer on a trawler (including research trawlers) in the Southeast Region, or have successfully completed a training course conducted or approved by the Director of the NMFS Southeast Fisheries Science Center. Observers will be state or federal employees or contracted observers working for another institution such as a university and assigned as needed.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological techniques or other forms of information technology.

The Southeast Region's Web site allows the public to view the manual for BRD testing. The Web site provides a suitable mechanism for dissemination of information via downloading of the manual. However, due to the complex nature of the testing and application process, the forms are not available on the Web site. Otherwise, no improved information technology has been identified as a practical means for reducing the burden on the public. The SEFSC has been involved in the testing process to assist and ensure the quality of the test. The information can be viewed at:
http://sero.nmfs.noaa.gov/sf/pdfs/Revisions%20to%20BRD%20and%20Testing%20Protocalls%20FR.pdf

4. Describe efforts to identify duplication.

The Magnuson-Stevens Act's operational guidelines require each FMP to evaluate existing state and Federal laws that govern the fisheries in question, and the findings are made part of each FMP. Each Fishery Management Councils membership is comprised of state and Federal officials responsible for resource management in their area. These two circumstances identify other collections that may be gathering the same or similar information. Data submitted to NMFS for BRD certification in Federal waters will be provided upon request to states so that the BRD can be certified in state waters. Similarly, data which are collected by or submitted to the states for BRD certification in state waters may be used by NMFS for Federal certification.

Each state in the region has an independent BRD testing procedure. Data collected for or by the state for their independent certification program is not part of the burden in this collection although that data may be used for federal certification. Burden time for the state to reproduce the data and forward it to NMFS is included in this submission. Burden time for a state to collect data under federal grant specifically to be submitted to NMFS for federal certification is part of this collection.

5. If the collection of information involves small businesses or other small entities, describe the methods used to minimize burden.

Because all applicants are considered small businesses, separate requirements based on size of business have not been developed. Only the minimum data to meet the analytical needs of the BRD testing protocols are requested from all applicants.

6. Describe the consequences to the Federal program or policy activities if the collection is not conducted or is conducted less frequently.

Reporting is at the request of the respondent. If this collection is not approved, there will be no procedure for approving new BRD developed by the shrimp industry or NMFS.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with OMB guidelines.

The collection is consistent with the guidelines.

8. Provide a copy of the PRA Federal Register Notice that solicited public comments on the information collection prior to this submission. Summarize the public comments received in response to that notice and describe the actions taken by the agency in response to those comments. Describe the efforts to consult with persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported.

A Federal Register Notice published on January 22, 2008 (73 FR 3696) solicited public comments. No comments were received.

9. Explain any decisions to provide payments or gifts to respondents, other than remuneration of contractors or grantees.

There are no payments or gifts to respondents.

10. Describe any assurance of confidentiality provided to respondents and the basis for assurance in statute, regulation, or agency policy.

All data that are submitted are treated as confidential in accordance with National Oceanic and Atmospheric Administration (NOAA) Administrative Order 216-100. Assurance is given on the forms.

Additional protections: Records are stored in computerized databases or compact discs (CD)s in locked rooms; paper records are stored in file folders in locked metal cabinets and/or locked rooms. Records are stored in buildings with doors that are locked during and after business hours. Visitors must register with security guards and must be accompanied by Federal personnel at all times. Records are organized and retrieved by NMFS internal identification

number, name of entity, permit number, vessel name or vessel identification number, or plant name. Electronic records are protected by a user identification/password. The user identification/password is issued to individuals as authorized by authorized personnel.

All electronic information disseminated by NOAA adheres to the standards set out in Appendix III, Security of Automated Information Resources, Office of Management and Budget (OMB) Circular A-130; the Computer Security Act; an the Government Information Security Reform Act and follows National Institute of Standards and Technology (NIST) SP 800-18, Guide for Developing Security Plans for Federal Information Systems; NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems; NIST SP 800-53, Recommended Security Controls for Federal Information Systems.

A Privacy Act System of Records Notice for all NMFS Sustainable Fisheries Permits was published on April 17, 2008 (73 FR 20914) and became effective June 11, 2008 (73 FR 33065).

11. Provide additional justification for any questions of a sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.

No questions of a sensitive nature are asked.

12. Provide an estimate in hours of the burden of the collection of information.

The estimated number of applicants is 28 per year. As described in the response to Question 2, the observers complete all documents other than the application letter and vessel information form and the gear specification form. Forms completed by the observer require only a signature from the respondent.

1. The reporting requirements for the BRD testing protocols consist of completing a vessel information form, a gear specification form, a station sheet BRD evaluation form, a length frequency form, a condition and fate form and conducting the test.

a. The estimated time to complete an application letter and vessel information form is 30 minutes; the gear specification form is 30 minutes**, a total of 14 hours for each** form (28 x 0.30).

b. The station sheets will require 2 hours per trip or a total of 14 hours (captain's signature is the only burden; at 1 minute per signature, the burden for 28 forms is 28 minutes**;** 30 tows with one form per tow = 30 x 28 x 1 minute/60 minutes = **14 hours**).

c. The species characterization form, again counting captain's signature only, adds **14 hours**: at 1 minute per signature, the burden for 28 forms is 28 minutes**;** 30 tows with one form per tow = 30 x 28 x 1 minute/60 minutes = **14 hours.**

d. The length frequency form, again counting captain's signature only, adds **14 hours**: at 1 minute per signature, the burden for 28 forms is 28 minutes**;** 30 tows with one form per tow = 30 x 28 x 1 minute/60 minutes = **14 hours**.

e. The condition and fate form, providing biological data, is completed upon sighting of a sea turtle, which is estimated to occur on about 25 per cent of the tests – in this case, 7 trips (7/28 = 0.25) – for a total of **7 minutes** (1 minute each for captain's signature).

.

2. The estimated time to complete one Trip Report/Cover Sheet for each trip = 1 minute for the captain's signature, or **28 minutes**.

In addition, we expect four independent BRD tests to be performed under the state programs per year, for an additional four respondents. The burden time associated with reproducing the test information and results is estimated at 5 minutes per application, or **20 minutes**.

The total time for all items above is (5 x 14 hours) + 7 minutes + 28 minutes + 20 minutes = 70 hours and 55 minutes, or 71 hours (rounded down to 70 hours in ROCIS).

Requirement	Respondents	Responses	Response Time (Hours)	Burden Time (Hours)
Application/Vessel Information Form	28	28	0.5	14
Gear Specification Form	28	28	0.5	14
Station Sheet BRD Evaluation Form	28	840	0.017	14
Species Characterization Form	28	840	0.017	14
Length Frequency Form	28	840	0.017	14
Condition and Fate Form	28	7	0.017	7 minutes
Trip Report/Cover Sheet	28	28	0.017	28 minutes
Independent BRD tests (duplication/mailing)	4	4	0.083	20 minutes
TOTALS	**32**	**2,615**		**71**

13. Provide an estimate of the total annual cost burden to the respondents or record-keepers resulting from the collection (excluding the value of the burden hours in #12 above).

The cost of duplication and mailing reports is $20 per applicant: 32 x $20 = $640 (rounded down to $639 in ROCIS).

A third party agent provides observers. Observers will be state or federal employees or contracted observers working for another institution such as a university. No cost is thus associated with the observer.

14. Provide estimates of annualized cost to the Federal government.

Tasks, e.g. review of forms submitted, are covered under normal duties of staff. Re cost of observers: observers may be NMFS employees, state employees (including university personnel), or employees/contractors of private organizations. The cost of the observer is paid by the observer provider, either through normal employment (wage/salary), or more likely from a research grant from either a state/federal/private source.

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB 83-I.

Adjustments: burden for tasks completed by observers had previously been included in error; formerly counted costs for observers are not applicable, thus decreasing the responses by 1,451 and hours by 1,733 and the costs by $338,336 (in ROCIS, the adjustment appears to be $338,361, as the total cost was rounded up to the nearest thousand when the ICR was migrated to ROCIS). Overall costs per respondent for duplication and submission of forms have not changed.

Program change: the test requirements for the Gulf and South Atlantic areas are now the same and thus no longer include pre-certification or species specification information for the Gulf; this program change results in a decreases in responses of 1,224 and hours of 5,096 for the 24 pre-certification forms.

Total change including adjustment and program change: 2,675 responses and 6,829 hours.

16. For collections whose results will be published, outline the plans for tabulation and publication.

Results will not be published except for the list of BRD that have been certified.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons why display would be inappropriate.

Not applicable.

18. Explain each exception to the certification statement identified in Item 19 of the OMB 83-I.

There are no exceptions.

B. COLLECTIONS OF INFORMATION EMPLOYING STATISTICAL METHODS

This collection does not use statistical methods.

BYCATCH REDUCTION DEVICE TESTING MANUAL

2008

National Marine Fisheries Service
Southeast Regional Office
263 13th Avenue South
St. Petersburg, Florida 33701

Galveston Laboratory
4700 Avenue U
Galveston, Texas 77551-5997

Mississippi Laboratories
Pascagoula Facility
3209 Frederic Street
Pascagoula, Mississippi 39568-1207

DEFINITIONS

Bycatch reduction criterion is the standard by which a BRD candidate will be evaluated. To be certified for use by the shrimp fishery in the Exclusive Economic Zone (EEZ) off the southeastern United States (North Carolina through Texas), the BRD candidate must demonstrate a successful reduction of total finfish bycatch by at least 30 percent by weight.

Bycatch reduction device (BRD) is any gear or trawl modification designed to allow finfish to escape from a shrimp trawl.

BRD candidate is a bycatch reduction device to be tested for certification for use in the commercial shrimp fishery of southeastern United States.

Certified BRD is a BRD that has been tested according to the procedure outlined herein and has been determined by the RA as having met the bycatch reduction criterion.

Control trawl means a trawl that is not equipped with a BRD during the evaluation.

Experimental trawl means the trawl that is equipped with the BRD candidate during an evaluation.

Evaluation and oversight personnel means scientists, observers, and other technical personnel who, by reason of their occupation or scientific expertise or training, are approved by the RA as qualified to evaluate and review the application and testing process.

Net/side bias means when the net(s) being fished on one side of the vessel demonstrate a different catch rate (fishing efficiency) than the net(s) being fished on the other side of the vessel during paired-net tests.

Observer means a person on the list maintained by the RA of individuals qualified to supervise and monitor a BRD certification test.

Paired-net test means a tow during certification trials where a control net and an experimental net are fished simultaneously, and the catches and catch rates between the nets are compared.

Provisional Certification Criterion means a secondary benchmark which would allow a BRD candidate to be used for a time-limited period in the southeastern shrimp fishery. To meet the criterion, the BRD candidate must demonstrate a successful reduction of total finfish bycatch by at least 25 percent by weight.

Provisionally certified BRD means a BRD that has been tested according to the procedure outlined herein and has been determined by the RA as having met the

provisional certification criterion. A BRD meeting the provisional certification criterion would be certified by the RA for a period of 2 years.

Regional Administrator (RA) means the Southeast Regional Administrator, National Marine Fisheries Service.

Required measurements refers to the quantification of gear characteristics such as the dimensions and configuration of the trawl, the BRD candidate, the doors, or the location of the BRD in relation to other parts of the trawl gear that are used to assess the performance of the BRD candidate.

Sample size means the number of successful tows (a minimum of 30 tows per test are required).

Shrimp trawler means any vessel that is equipped with one or more trawl nets whose on-board or landed catch of shrimp is more than 1 percent, by weight, of all fish comprising its on-board or landed catch.

Successful tow means that the control and experimental trawl were fished in accordance with the requirements set forth herein and the terms and conditions of the letter of authorization, and there is no indication problematic events, such as those listed in Appendix D-5, occurred during the tow to impact or influence the fishing efficiency (catch) of one or both nets.

Tow time means the total time (hours and minutes) an individual trawl was fished (i.e., the time interval beginning when the winch is locked after deploying the net overboard, and ending when retrieval of the net is initiated).

Trawl means a net and associated gear and rigging used to catch shrimp. The terms trawl and net are used interchangeably throughout the manual.

Try net means a separate net pulled for brief periods by a shrimp trawler to test for shrimp concentrations or determine fishing conditions (e.g., presence of absence of bottom debris, jellyfish, bycatch, seagrasses).

Tuning a net means adjusting the trawl and its components to minimize or eliminate any net/side bias that exists between the two nets that will be used as the control and experimental trawls during the certification test.

I. Introduction

This Bycatch Reduction Device Testing Manual (Manual) establishes a standardized process for evaluating the ability of bycatch reduction device (BRD) candidates to meet the established bycatch reduction criterion, and be certified for use in the Exclusive Economic Zone (EEZ) by the southeastern shrimp fishery. BRDs are required for use in shrimp trawls fished shoreward of the 100-fathom (183-meter) depth contour in the Gulf of Mexico, and within the EEZ of the South Atlantic region.

Various BRD requirements also exist in state waters in the South Atlantic and off Florida and Texas in the Gulf of Mexico. Persons wishing to conduct BRD candidate evaluations exclusively in state waters do not need to apply to the National Marine Fisheries Service (NOAA Fisheries Service) for authorization to conduct these tests, but should contact the appropriate state officials for authorizations. However, for data collected in such evaluations to be considered by NOAA Fisheries Service for certification, the operations plan and data collection procedures must meet the criteria established in this Manual.

II. BRD Candidate Evaluations

A. Application

Persons interested in evaluating the efficiency of a BRD candidate must apply for, receive, and have on board the vessel during the evaluation, a Letter of Authorization (LOA) from the Regional Administrator (RA). To receive an LOA, the applicant must submit the following documentation to the RA: (1) a completed application form (Appendix A); (2) a brief statement of the purpose and goal of the activity for which the LOA is requested; (3) an operations plan (see Section C below) describing the scope, duration, dates, and location of the test, and methods that will be used to conduct the test; (4) an 8.5-inch x 11-inch (21.6-cm x 27.9-cm) diagram drawn to scale of the BRD design; (5) an 8.5-inch x 11-inch (21.6-cm x 27.9-cm) diagram drawn to scale of the BRD in the shrimp trawl; (6) a description of how the BRD is supposed to work; (7) a copy of the testing vessel's U.S. Coast Guard documentation or its state registration; and (8) a copy of the testing vessel's Federal commercial shrimp vessel permit.

An applicant requesting an LOA to test an unapproved turtle excluder device (TED) as a BRD (including modifications to a TED that would enhance finfish exclusion) must first apply for and obtain from the RA an experimental TED authorization pursuant to 50 CFR 223.207(e)(2). Applicants should contact the Protected Resources Division of NOAA Fisheries Service's Southeast Regional Office for further information. The LOA applicant must include a copy of that authorization with the application.

Incomplete applications will be returned to the applicant along with a letter from the RA indicating what actions the applicant may take to make the application complete.

There is no cost to the applicant for the RA's administrative expenses such as reviewing applications, issuing LOAs, evaluating test results, or certifying BRDs. However, all other costs associated with the actual testing activities are the responsibility of the applicant, or any associated sponsor.

If an application for an LOA is denied, the RA will provide a letter of explanation to the applicant, together with relevant recommendations to address the deficiencies that resulted in the denial.

B. Allowable Activities

Issuance of an LOA to test a BRD candidate in the South Atlantic or Gulf of Mexico allows the applicant to remove or disable the existing certified BRD in one outboard net (to create a control net), and to place the BRD candidate in another outboard net in lieu of a certified BRD (to create an experimental net). All other trawls under tow during the test must have a certified BRD, unless these nets are specifically exempted in the LOA. All trawls under tow during the test must have an approved TED unless operating under an authorization issued pursuant to 50 CFR 223.207(e)(2), whereby the test is being conducted on an experimental TED. The LOA, and experimental TED authorization if applicable, must be on board the vessel while the test is being conducted. The term of the LOA will be 60 days; should circumstances require a longer test period, the applicant may apply to the RA for a 60-day extension.

C. Operations Plan

An operations plan should be submitted with the application describing a method to compare the catches of shrimp and fish in a control net (net without a BRD candidate installed) to the catches of the same species in an experimental net (a net configured identically to the control net but also equipped with the BRD candidate).

The applicant may choose to conduct a pre-certification test of a prototype BRD candidate. A pre-certification test would be conducted when the intent is to assess the preliminary effectiveness of a prototype BRD candidate under field conditions, and to make modifications to the prototype BRD candidate during the field test. For pre-certification testing, the operations plan must include only a description of the scope, duration, dates, and location of the test, along with a description of methods that will be used to conduct the test. No observer is required for a pre-certification test, but the applicant may choose to use an observer to maintain a written record of the test. The applicant will maintain a written record for both the control and experimental net during each tow. Mandatory data collection is limited to the weight of the shrimp catch and the weight of the total finfish catch in each test net during each tow. These data must be submitted to NOAA Fisheries Service at the conclusion of the test. Although not required, the applicant may wish to incorporate some or all the certification test requirements listed below.

For a BRD candidate to be considered for certification, the operations plan must be more detailed and address the following topics:

- The primary assumption in assessing the bycatch reduction efficiency of the BRD candidate during paired-net tests is that the inclusion of the BRD candidate in the experimental net is the only factor causing a difference in catch from the control net. Therefore, the nets to be used in the tests must be calibrated (tuned) to minimize, to the extent practicable, any net/side bias in catch efficiency prior to beginning a test series, and tuned again after any gear modification or change. Additional information on tuning shrimp trawls to minimize bias is available from the Harvesting Technology Branch, Mississippi Laboratories, Pascagoula Facility, 3209 Frederic Street, Pascagoula, Mississippi 39568-1207; phone (601) 762-4591.

- A standard tow time for a proposed evaluation should be defined. Tow times must be representative of the tow times used by commercial shrimp trawlers. The applicant should indicate what alternatives will be considered should the proposed tow time need adjustment once the test begins.

- A minimum sample size of 30 successful tows using a specific BRD candidate design is required for the statistical analysis described in Section F. No alterations of the BRD candidate design are allowed during a specific test series. If the BRD candidate design is altered, a new test series must be started. If a gear change (i.e., changing nets, doors, or rigging) is required, the nets should be tuned again before proceeding with further tests to complete the 30-tow series. Minor repairs to the gear (e.g., sewing holes in the webbing; replacing a broken tickler chain with a new one of the same configuration) are not considered a "gear change."

- For tests conducted on twin-rig vessels, biases that might result from the use of a try net should be minimized. Total fishing times for a try net must be a consistent percentage of the total tow time during each tow made in the test.

- To incorporate any potential net/side bias that remains after the tuning tows (e.g., the effect of a try net), or to accommodate for bias that develops between the control and experimental nets during the test, the operations plan should outline a timetable ensuring that an equal number of successful tows are made with the BRD candidate employed in both the port and starboard nets.

- Mandatory data to be collected during a test includes: (1) detailed gear specifications as set forth in Appendices B and C, and (2) pertinent information concerning the location, duration and catch from individual tows as set forth in Appendices D and F.

- Following each paired tow, the catches from the control and experimental nets must be examined separately. This requires that the catch from each net be kept separate from each other, as well as from the catch taken in other nets fished during that tow. Mandatory data collections include recording the weight of the total catch of each test net (control and experimental nets), the catch of shrimp (i.e., brown, white, pink, rock, or other shrimp by species) in each test net, and the catch of total finfish in aggregate in each test net.

- When recording the detailed information on the species found in the catch, if the catch in a net does not fill one standard 1-bushel [ca. 10 gallon] (30 liters) polyethylene shrimp basket (ca. 70 pounds) (31.8 kg), but the tow is otherwise considered successful, data must be collected on the entire catch of the net, and recorded as a "select" sample (see Appendices D and F), indicating that the values represent the total catch of the particular net. If the catch in a net exceeds 70 pounds (31.8 kg), a well-mixed sample consisting of one standard 1-bushel [ca. 10 gallon] (30 liters) polyethylene shrimp basket must be taken from the total catch of the net. The total weight of the sample must be recorded, as well as the weights (and numbers as applicable) of the various species or species groups found within that sample. These sample values can then be extrapolated to estimate the quantity of those species or species groups found in the total catch of the particular net.

- Although not a criterion for certification, applicants testing BRD candidates are encouraged to collect additional information that may be pertinent to addressing bycatch issues in their respective regions. For example, in the western Gulf of Mexico applicants are especially encouraged to collect information on red snapper. If the applicant chooses to collect these data, the total ("select") catch of the target species from each test net (not just from the sample) should be recorded along with lengths for as many individuals per net per tow as set forth in Appendices E and F. Additional information in regard to the catch can be recorded on forms such as Appendix G.

The operations plan should address what the applicant will do should it become necessary to deviate from the primary procedures outlined in the operations plan. The plan should describe in detail what will be done to continue the test in a reasonable manner that is consistent with the primary procedures. For example, it may become necessary to alter the pre-selected tow time to adapt to local fishing conditions to successfully complete the test. Prior to issuing a LOA, the RA may consult with evaluation personnel review the acceptability of these proposed alterations.

D. Observer Requirement

It is the responsibility of the applicant to ensure that a qualified observer is on board the vessel during the certification tests. A list of qualified observers is available from the RA. Observers may include employees or individuals acting on behalf of NOAA

Fisheries Service, state fishery management agencies, universities, or private industry, who meet the minimum requirements outlined in Appendix H. Any change in information or testing circumstances, such as replacement of the observer, must be reported to the RA within 30 days. Under 50 CFR 600.746, when any fishing vessel is required to carry an observer as part of a mandatory observer program under the Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 1801, *et seq.*), the owner or operator of the vessel must comply with guidelines, regulations, and conditions to ensure their vessel is adequate and safe to carry an observer, and to allow normal observer functions to collect information as described in this Manual. A vessel owner is deemed to meet this requirement if the vessel displays one of the following: (i) a current Commercial Fishing Vessel Safety Examination decal, issued within the last 2 years, that certifies compliance with regulations found in 33 CFR, chapter I, and 46 CFR, chapter I; (ii) a certificate of compliance issued pursuant to 46 CFR 28.710; or (iii) a valid certificate of inspection pursuant to 46 U.S.C. 3311. The observer has the right to check for major safety items, and if those items are absent or unserviceable, the observer may choose not to sail with the vessel until those deficiencies are corrected.

E. Reports

A report on the BRD candidate test results must be submitted by the applicant or associated sponsor before the RA will consider the BRD for certification. The report must contain a comprehensive description of the tests, copies of all completed data forms used during the tests, and photographs, drawings, and similar material describing the BRD. The captain, vessel owner, or the applicant must sign and submit the cover form (Appendix I). The report must include a description and explanation of any unanticipated deviations from the operations plan which occurred during the test. These deviations must be described in sufficient detail to indicate the tests were continued in a reasonable manner consistent with the approved operations plan procedures. Applicants must provide information on the cost of materials, labor, and installation of the BRD candidate. In addition, any unique or special circumstances of the tests, such as special operational characteristics or fishing techniques which enhance the BRD's performance, should be described and documented as appropriate.

F. Certification

The RA will determine whether the required reports and supporting materials are sufficient to evaluate the BRD candidate's efficiency. The determination of sufficiency would be based on whether the applicant adhered to the prescribed testing procedure or provided adequate justification for any deviations from the procedure during the test. If the RA determines that the data are sufficient for evaluation, the BRD candidate will be evaluated to determine if it meets the bycatch reduction criterion. In making a decision, the RA may consult with evaluation and oversight personnel. Based on the data submitted for review, the RA will determine the effectiveness of the BRD candidate, using appropriate statistical procedures such as Bayesian analyses, to determine if the BRD candidate meets the following conditions:

#1) There is at least a 50-percent probability that the true reduction rate of the BRD candidate meets the bycatch reduction criterion (i.e., the BRD candidate demonstrates a best point estimate [sample mean] that meets the certification criterion); and

#2) There is no more than a 10-percent probability that the true reduction rate of the BRD candidate is more than 5 percentage points less than the bycatch reduction criterion.

To be certified for use in the fishery, the BRD candidate will have to satisfy both criteria. The first condition ensures that the observed reduction rate of the BRD candidate has an acceptable level of certainty that it meets the bycatch reduction criterion. The second condition ensures the BRD candidate demonstrates a reasonable degree of certainty the observed reduction rate represents the true reduction rate of the BRD candidate. This determination ensures the operational use of the BRD candidate in the shrimp fishery will, on average, provide a level of bycatch reduction that meets the established bycatch reduction criterion. Interested parties may obtain details regarding the hypothesis testing procedure to be used by contacting the Harvesting Technology Branch, Mississippi Laboratories, Pascagoula Facility, 3209 Frederic Street, Pascagoula, Mississippi 39568-1207; phone (228) 762-4591. Following a favorable determination of the certification analysis, the RA will certify the BRD (with any appropriate conditions as indicated by test results) and publish the notice of certification in the *Federal Register*.

In addition, based on the data provided, the RA may provisionally certify a BRD candidate based on the following condition:

#1) There is at least a 50-percent probability that the true reduction rate of the BRD candidate is no more than 5 percentage points less than the bycatch reduction criterion (i.e., the BRD candidate demonstrates a best point estimate [sample mean] within 5 percentage points of the certification criterion).

A provisional certification will be effective for 2 years from the date of publication of a notice in the *Federal Register* announcing this provisional certification. This time period will allow additional wide scale industry evaluation of the BRD candidate, during which additional effort would be made to improve the efficiency of the BRD to meet the certification criterion.

III. BRDs Not Certified and Resubmission Procedures

The RA will advise the applicant, in writing, if a BRD is not certified. This notification will explain why the BRD was not certified and what the applicant may do to either modify the BRD or the testing procedures to improve the chances of having the BRD certified in the future. If certification was denied because of insufficient information, the RA will explain what information is lacking. The applicant must provide the additional information within 60 days from receipt of such notification. If the RA subsequently certifies the BRD, the RA will announce the certification in the *Federal Register*.

IV. Decertification of BRDs

The RA will decertify a BRD whenever NOAA Fisheries Service determines a BRD no longer satisfies the bycatch reduction criterion. Before determining whether to decertify a BRD, the RA will notify the appropriate Fishery Management Council in writing, and the public will be provided an opportunity to comment on the advisability of any proposed decertification. The RA will consider any comments from the Council and public, and if the RA elects to proceed with decertification of the BRD, the RA will publish proposed and final rules in the *Federal Register* with a comment period of not less than 15 days on the proposed rule.

V. Interactions with sea turtles

The following section is provided for informational purposes. Sea turtles are listed under the Endangered Species Act as either endangered or threatened. The following procedures apply to incidental take of sea turtles under 50 CFR 223.206(d)(1):

"Any sea turtles taken incidentally during the course of fishing or scientific research activities must be handled with due care to prevent injury to live specimens, observed for activity, and returned to the water according to the following procedures:

> A) Sea turtles that are actively moving or determined to be dead (as described in paragraph (B)(4) below) must be released over the stern of the boat. In addition, they must be released only when fishing or scientific collection gear is not in use, when the engine gears are in neutral position, and in areas where they are unlikely to be recaptured or injured by vessels.
>
> B) Resuscitation must be attempted on sea turtles that are comatose or inactive by:
>
> > (1) Placing the turtle on its bottom shell (plastron) so that the turtle is right side up and elevating its hindquarters at least 6 inches (15.2 cm) for a period of 4 to 24 hours. The amount of elevation depends on the size of the turtle; greater elevations are needed for larger turtles. Periodically, rock the turtle gently left to right and right to left by holding the outer edge

of the shell (carapace) and lifting one side about 3 inches (7.6 cm) then alternate to the other side. Gently touch the eye and pinch the tail (reflex test) periodically to see if there is a response.

(2) Sea turtles being resuscitated must be shaded and kept damp or moist but under no circumstance be placed into a container holding water. A water-soaked towel placed over the head, carapace, and flippers is the most effective method in keeping a turtle moist.

(3) Sea turtles that revive and become active must be released over the stern of the boat only when fishing or scientific collection gear is not in use, when the engine gears are in neutral position, and in areas where they are unlikely to be recaptured or injured by vessels. Sea turtles that fail to respond to the reflex test or fail to move within 4 hours (up to 24, if possible) must be returned to the water in the same manner as that for actively moving turtles.

(4) A turtle is determined to be dead if the muscles are stiff (rigor mortis) and/or the flesh has begun to rot; otherwise, the turtle is determined to be comatose or inactive and resuscitation attempts are necessary.

Any sea turtle so taken must not be consumed, sold, landed, offloaded, transshipped, or kept below deck."

OMB No. 0648-0345 Form Approval Expires: 06/30/2008

U.S. DEPT OF COMMERCE, NOAA
National Marine Fisheries Service, Southeast Region
263 13th Avenue South
St. Petersburg, FL 33701

APPENDIX A - APPLICATION TO TEST A BYCATCH REDUCTION DEVICE IN THE EXCLUSIVE ECONOMIC ZONE

☐ Pre Certification ☐ Certification

FOR OFFICE USE ONLY	
Expiration Date:	
Reviewer Initials and Date	
Violation Number and Hold Date	
Violation Clear Date and Clearers initials:	
Non Reporting Hold Date	
Non Reporting Cleared Date	

SECTION 1. VESSEL INFORMATION (please type)

VESSEL NAME	CG SAFETY STICKER NO.	USCG DOCUMENT NUMBER or STATE REGISTRATION NUMBER	
HOMEPORT - CITY AND STATE	ENGINE HORSEPOWER	LENGHT(IN FEET)	HOLD CAPACITY (TONS)

SECTION 2. APPLICANT INFORMATION

OWNER'S NAME	AREA/CODE TELEPHONE		
MAILING ADDRESS			
CITY	STATE	ZIP CODE	DATE OF BIRTH: MONTH - DAY - YEAR
TIN (EIN or SSN)			

SECTION 3. OWNER/OPERATOR INFORMATION IF REQUIRED: See instructions for requirements

OWNER'S NAME	AREA/CODE TELEPHONE		
MAILING ADDRESS			
CITY	STATE	ZIP CODE	DATE OF BIRTH: MONTH - DAY - YEAR
TIN (EIN or SSN)			

SECTION 4. LEASE INFORMATION: See instructions for requirements

OWNER'S NAME	AREA/CODE TELEPHONE		
MAILING ADDRESS			
CITY	STATE	ZIP CODE	LEASE EXPIRATION - MONTH - DAY - YEAR

SECTION 5. SIGNATURE (ALL APPLICATIONS MUST BE SIGNED)

Applicant's Signature	Applicant's Position	Date
Owner's Signature (if different from Applicant	Position - if owner is a business	Date

GENERAL INSTRUCTIONS

Under 50 CFR part 622.41(g), a person who proposes a bycatch reduction device (BRD) for pre-certification or for certification for use in the southeastern shrimp fishery must submit this application to test a BRD, conduct the testing, and submit the results of the test in accordance with the **Bycatch Reduction Device Testing Manual**. A BRD that meets the certification criterion, as determined under the testing protocol, will be added to the list of certified BRDs.

1. Type or print legibly in ink. Incomplete or unreadable applications will be returned.

2. Each application must be accompanied by a copy of the vessel's CURRENT Coast Guard certificate of documentation or, if not documented, its state registration certificate; and a test plan showing: (1) an 8.5" x 11" diagram drawn to scale of the BRD; (2) an 8.5" x 11" diagram drawn to scale of the BRD and turtle excluder device in the shrimp trawl; (3) a description of how the BRD is supposed to work; (4) the results of previous tests including but not limited to location, time, and area where tested; (5) the location, time, and area where the proposed tests would take place; and (6) the identify of the qualified observer (for certification phase testing only), and a basis for the observer's qualifications.

3. Mail the application, and copy of documentation/registration to: NMFS , 263 13th Avenue South, St. Petersburg, FL, 33701. Questions may be phoned to (727) 824-5305 between 8:00 am and 4:30 pm, eastern time.

4. Additional copies of this **application** and the **Bycatch Reduction Device Testing Manual** are available from NMFS at the address in

APPLICATION INSTRUCTIONS

SECTION 1 Enter name, official number and length of vessel as they appear on the certificate of documentation or, if not documented, on the state registration certificate. Enter Coast Guard Vessel Safety number. Under "Home Port", enter the city and state where the vessel is customarily kept, not necessarily the home port on a certificate of documentation. The vessel owner must display a current vessel safety sticker from the Coast Guard, before NMFS will assign an observer.

SECTION 2 Provide the name, address, telephone number and other identifying information of the applicant.

SECTION 3 COMPLETE THIS SECTION ONLY IF THE OWNER / OPERATOR IS DIFFERENT THAN THE APPLICANT. Any change in the information in Section 3 must be reported to the Regional Administrator within 30 days after such change.

SECTION 4 COMPLETE THIS SECTION ONLY WHEN THE VESSEL IS BEING OPERATED UNDER A LEASE OR OTHER WRITTEN MANAGEMENT AGREEMENT THAT BESTOWS CONTROL OVER THE DESTINATION, FUNCTION OR OPERATION OF THE VESSEL TO A PERSON OTHER THAN THE PERSON SHOWN IN SECTION 2. Provide the name, address, telephone number and other identifying information of the controlling person. Enter the date of expiration of the lease or written management agreement that transferred control of the vessel from the person shown in Section 2. If such lease or written management agreement exists, the controlling person is the owner for the purposes of the authorization. Any change in the information in Section 4 must be reported to the Regional Administrator within 30 days after such change.

SECTION 5 ALL APPLICATIONS MUST BE SIGNED OTHERWISE IT WILL BE RETURNED.

The NMFS requires this collection of information to minimize the bycatch of finfish in the southeastern shrimp fishery. The data and testing will be used to develop improved bycatch reduction devices (BRDs). Responses are required under the Magnuson-Stevens Act to obtain certification that allows use of a BRD in the shrimp fishery. Data will be confidential pursuant to the Magnuson-Stevens Act and other applicable law. Notwithstanding any other provisions of the law, no person is required to, nor shall any person be subject to a penalty to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Public reporting burden for this collection of information is estimated to average 140 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other suggestions for reducing this burden to National Marine Fisheries Service, 263 13th Avenue South, St. Petersburg, FL 33701. OMB No. 068-0345

OMB No. 0648 -0345 Approval Expires - 06/30/2008

APPENDIX B

GEAR SPECIFICATION FORM
BRD TESTING PROTOCOL

Gear ID # ☐ Control (C) or Experimental (E) ☐

ORG PRO# / TRIP NO. ☐☐☐☐☐ VESSEL ☐☐☐ TOW NO. ☐☐☐ MO DY YR DATE ☐☐☐☐☐☐ NET POSITION ☐

SECTION I NET GEAR MEASUREMENTS

NET TYPE AND HEAD/FOOTROPE MEASUREMENTS

Net Type ☐☐☐☐☐☐☐☐☐☐

Headrope Length ☐☐☐☐☐ Feet

Footrope Length ☐☐☐☐☐ Feet

Comments _____

LEG LINE MEASUREMENTS

Top Leg Length ☐☐.☐☐ Feet

Bottom Leg Length ☐☐.☐☐ Feet

Top Leg Dummy ☐☐.☐☐ Feet

Bottom Leg Dummy ☐☐.☐☐ Feet

TRAWL BODY

Type Nylon ☐ Poly ☐ Spectra ☐

Mesh Size ☐☐.☐☐ Inches

Comments _____

TRAWL EXTENSION

Type Nylon ☐ Poly ☐ Spectra ☐

Mesh Size ☐☐.☐☐ Inches

Comments _____

COD END

Type Nylon ☐ Poly ☐ Spectra ☐

Mesh Size ☐☐.☐☐ Inches Twine Size ☐☐

Comments _____

CHAFFING GEAR

Type Whiskers ☐ Mesh ☐ Metal ☐

_____

DOORS

Type Aluminum ☐ Wood ☐ Other ☐

Door Length ☐☐☐.☐ Feet

Door Height ☐☐☐.☐ Feet

Dummy Door Length ☐☐☐.☐ Feet

Comments _____

TICKLER CHAIN

Chain Length ☐☐☐☐.☐ Feet

Chain Size (guage) ☐☐.☐☐ Inches

Comments _____

LAZY LINE

Rigging: Elephant Ears ☐ Choke ☐

Comments

SECTION II BRD MEASUREMENTS

BRD TYPE Fisheye ☐ Jones Davis ☐ Other ☐☐☐☐☐☐☐☐☐☐

Fisheye position: Top ☐ Offset ☐

Codend length (# of meshes): ☐☐☐

Circumference of the codend (# of meshes): ☐☐☐

Distance of escape opening from elephant ear or choke rings: ☐☐ Feet ☐☐ Inches

Distance of escape opening from tie off rings: ☐☐ Feet ☐☐ Inches

Number of meshes the fisheye is offset from top center ☐☐

Fisheye (BRD) escape opening: Height ☐☐☐.☐☐ Inches Width ☐☐☐.☐☐ Inches

Shape of the escape opening: oval, diamond, square, halfmoon, if other

Specify ☐☐☐☐☐☐☐☐☐☐

Looking from the mouth of the net, is the BRD located in front of, at, or behind the point of attachment of the elephant ears: (check one) Front ☐ at ☐ Behind ☐

What is the length of the elephant ear from the point of attachment to the tip of the ring: ☐☐☐ Inches

Distance from point of attachment of elephant ear to tie off rings ☐☐ Feet ☐☐ Inches

REVISED 08/31/99

INSTRUCTIONS FOR THE GEAR SPECIFICATION FORM BRD TESTING PROTOCOL

A Gear Specification Form must be completed once for each net used in the control and experimental net positions during trawling operations. The control and experimental net positions should be changed every other day and a gear specification forms should be completed. If any gear setting or configuration changes are made, then additional form(s) must be completed by the observer for the affected net(s). If either of the two test nets is torn and repaired, then the repaired net must be remeasured for possible changes. All measurements should be recorded in feet and/or inches. Measurements should be converted to decimal form prior to data entry (10 feet and 6 inches = 10.5 feet, 3/4 inch = 0.75 inch). Detailed instructions for the Gear Specification Form are as follows:

TRIP NO.: Enter the Trip number. The organization will provide this information to the observer prior to their departure from port.

VESSEL: Enter the vessel code.

TOW NUMBER: Enter the starting tow number for a given vessel. If net or gear changes are made, enter the tow number when these changes occurred.

DATE: Enter the starting tow number date, or the date when the changes occurred.

NET POSITION: Enter 1 for outside port net; 2 for inside port net; 3 for inside starboard net; or 4 for outside starboard net. If there are only two nets being towed, the nets will be identified as nets numbered 2 and 3.

CONTROL - EXPERIMENTAL: Enter "C" for control net , this net will always closed or "E" for experimental net, the BRD is always open.

NET TYPE AND MEASUREMENTS
NET TYPE

NET TYPE: semi-balloon, balloon, flat, mongoose, etc.

HEADROPE LENGTH: Measure the length of the trawl headrope (feet and inches) where webbing is attached.

FOOTROPE LENGTH: Measure the length of the trawl footrope (feet and inches) where webbing is attached.

COMMENTS: (I.E.: Changed net type, replaced cut headrope or footrope).

LEG LINE

TOP LEGLINE LENGTH ON DOOR: Measure the length of the top legline (feet and inches) on the trawl's standard door. Top legline length is measured from the point of cable attachment at the door to the point where the first mesh on the net is tied to the cable.

BOTTOM LEGLINE LENGTH ON DOOR: Measure the length of the bottom legline (feet and inches) on the trawl's standard door. Bottom legline length is measured from the point of cable attachment at the door to the point where the first mesh on the net is tied to the cable.

TOP LEGLINE LENGTH ON DUMMY DOOR: Measure the top legline length (feet and inches) on the trawl's dummy door.

BOTTOM LEGLINE LENGTH ON DUMMY DOOR: Measure the bottom legline length (feet and inches) on the trawl's dummy door.

TWINE, MESH, AND OTHER GEAR MEASUREMENTS

TRAWL BODY

TYPE - Select the appropriate answer, nylon, poly or spectra.
MESH SIZE - Measure the stretched length to the nearest 1/4".
COMMENTS - (i.e., Changed net).

TRAWL EXTENSION

TYPE - Circle the appropriate answer, nylon, poly or spectra.
MESH SIZE - Measure the stretched length to the nearest 1/4".
COMMENTS -

COD END

TYPE - Circle the appropriate answer, nylon, poly or spectra.
MESH SIZE - Measure to nearest 1/4".
COMMENTS -

CHAFFING GEAR

TYPE - Select the appropriate answer; plastic, mesh or metal.
COMMENTS - (i.e., none used).

DOORS

DOOR TYPE - Select the appropriate answer, aluminum, wood or other.
If other, identify it in the comments section.
DOOR LENGTH - Measure the length of door (feet and inches).
DOOR HEIGHT - Measure the height of the door (feet and inches).
DUMMY DOOR LENGTH - Enter the length of the dummy door (feet and inches).
COMMENTS - any appropriate information on the doors.

TICKLER CHAIN

CHAIN LENGTH - Measure the length of the chain (feet and inches) from door to door.
CHAIN SIZE - Measure the length of the metal part of the link to the nearest 1/16 inch (do not measure the area where it is connected to another link or an area that has been welded).

COMMENTS - any appropriate information on the chain (i.e., replaced).

LAZY LINE

RIGGING - Select one, Elephant ears or Choke.
COMMENTS - any appropriate information on its use

TURTLE EXCLUDER DEVICE

TED TYPE - Enter Hard or Soft type.
TOP OR BOTTOM OPENING - Self explanatory.
COMMENTS - any appropriate information on its use

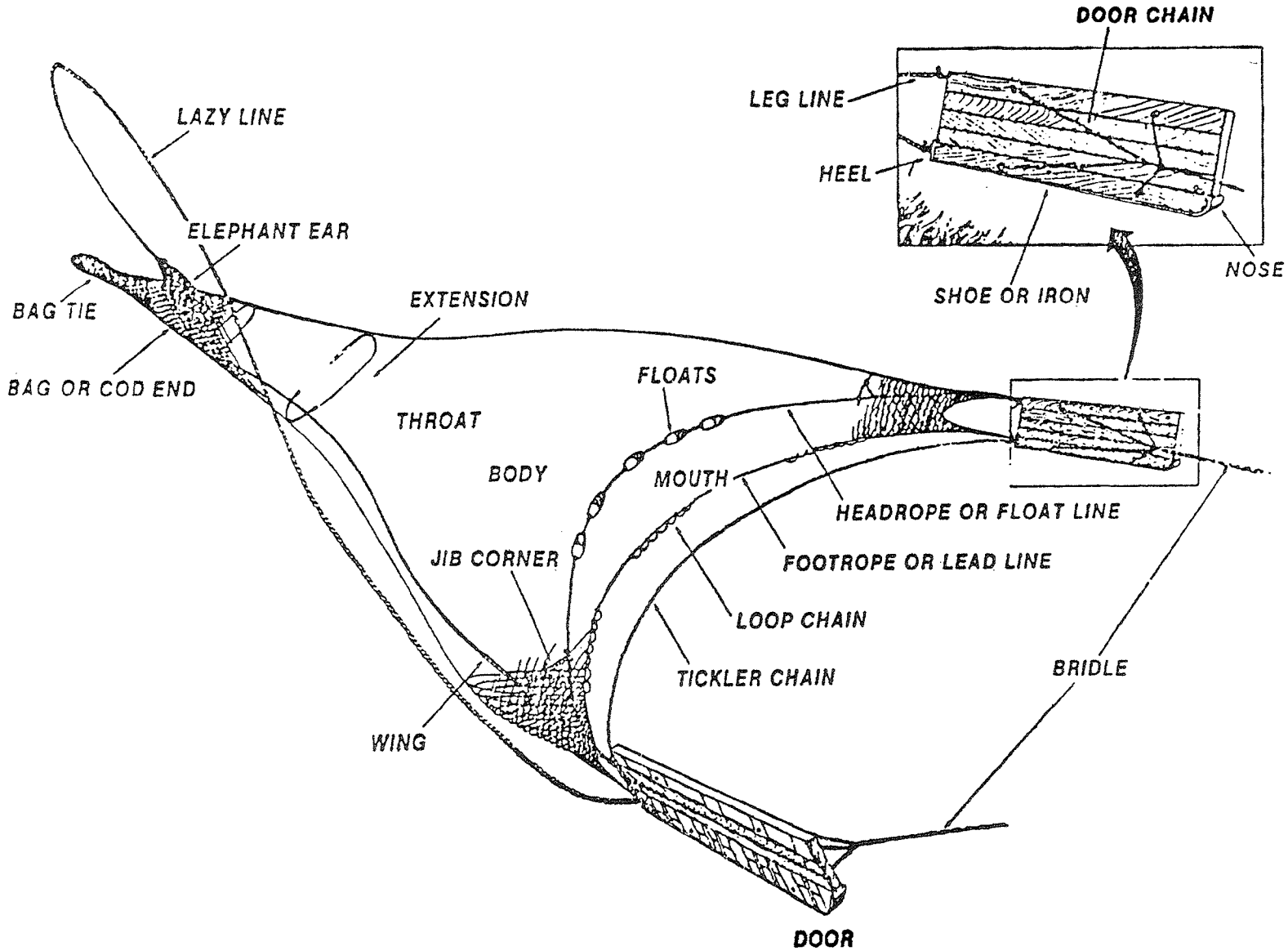
BYCATCH REDUCTION DEVICE (BRD)

TYPE - Select BRD type (i.e., Fisheye, Jones Davis or other).
FISHEYE - Select one by the location it is installed on the trawl net, top or offset.
CODEND LENGTH: Count the number of meshes in the length of the tailbag (codend) of the net.
MESHES IN CIRCUMFERENCE OF THE CODEND: Number of meshes in the circumference of the cod end.
DISTANCE OF ESCAPE OPENING FROM ELEPHANT EAR OR CHOKE RINGS: Measured in feet and inches.
DISTANCE OF ESCAPE OPENING FROM TIE OFF RINGS: Measured in feet and inches.
NUMBER OF MESHES THE FISHEYE IS OFFSET FROM TOP CENTER: Self explanatory.
FISHEYE ESCAPE OPENING: Measure the height and width
SHAPE OF THE ESCAPE OPENING: Write the shape in the squares marked "specify".
POSITION: Looking from the mouth of the net, is the BRD in front, centered or behind the elephant ears. (select one).
LENGTH OF ELEPHANT EAR: Measure, starting where the elephant ear is attached to the net to the tip of the ring (This is in inches).
SKETCH the fisheye including height and width on the back of the form being used to file your report and if possible make a cardboard outline of the opening.

The NMFS requires this collection of information to minimize the bycatch of finfish in the southeastern shrimp fishery. The data and testing will be used to develop improved bycatch reduction devices (BRDs). Responses are required under the Magnuson-Stevens Act to obtain certification that allows use of a BRD in the shrimp fishery of the Gulf of Mexico. Data will be confidential pursuant to the Magnuson-Stevens Act and other applicable law. Notwithstanding any other provisions of the law, no person is required to, nor shall any person be subject to a penalty to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Roy E. Crabtree, Southeast Regional Office, National Marine Fisheries Service, 263 13th Avenue South, St. Petersburg, FL 33701.

OTTER TRAWL COMPONENTS



APPENDIX C

OMB No. 0648 -0345 Approval Expires - 06/30/2008

TED/BRD SPECIFICATION FORM
BRD TESTING PROTOCOL

ORG PRO | TRIP NO. | VESSEL | TOW NO. | MO DY YR | DATE | NET POSITION

SECTION III — **TED MEASUREMENTS**

TED TYPE ☐ SOFT ☐ HARD

TED DESIGN (Circle one) WEEDLESS CURVED BAR STRAIGHT BAR UNKNOWN

TED OPENING ☐ TOP ☐ BOTTOM

TED FUNNEL (YES OR NO) ☐ **TED MATERIAL**

TED FLAP (YES OR NO) ☐ **# OF TED FLOATS**

TED ANGLE (DEGREES) **FLOAT TYPE**

TED DIMENSIONS LENGTH (INCHES) WIDTH (INCHES)

GEAR DESCRIPTIONS

BRD DESCRIPTION

BRD DIAGRAM

Sketch fisheye including height and width (on the back of this form) or attact cardboard outline (if possible).

GEAR DESCRIPTION

GEAR DIAGRAM

REVISED 08/31/99

INSTRUCTIONS FOR THE TED/BRD SPECIFICATION FORM BRD TESTING PROTOCOL

A TED/BRD Specification Form must be completed once for each net used in the control and experimental net positions during trawling operations. If any gear setting or configuration changes are made, then additional form(s) must be completed by the observer for the affected net(s). If either of the two test nets is torn and repaired, then the repaired net must be remeasured for possible changes. All measurements should be recorded in feet and/or inches. Measurements should be converted to decimal form prior to data entry (10 feet and 6 inches = 10.5 feet, 3/4 inch = 0.75 inch). Detailed instructions for the Gear Specification Form are as follows:

TRIP NO.: Enter the Trip number. The organization will provide this information to the observer prior to their departure from port.

VESSEL: Enter the vessel code.

TOW NUMBER: Enter the starting tow number for a given vessel. If net or gear changes are made, enter the tow number when these changes occurred.

DATE: Enter the starting tow number date, or the date when the changes occurred.

NET POSITION: Enter 1 for outside port net; 2 for inside port net; 3 for inside starboard net; or 4 for outside starboard net. If there are only two nets being towed, the nets will be identified as nets numbered 2 and 3.

CONTROL - EXPERIMENTAL: Enter "C" for control net , this net will always closed or "E" for experimental net, the BRD is always open.

TED:

TED TYPE -
Circle the appropriate answer, hard or soft.
Circle the appropriate answer, weedless, curved bar, or straight.
Circle the appropriate answer, top opening or bottom opening.
Circle the appropriate answer, TED funnel or no TED funnel.
Circle the appropriate answer, TED flap or no TED flap.

ANGLE OF TED (in degrees) - Measure angle of TED in trawl.

SIZE OF TED - Specify dimensions of TED used in both control and BRD trawl.

MATERIAL - Identify what material TED is constructed of.

FLOATATION - List number and type of floats used.

BYCATCH REDUCTION DEVICE (BRD):

DETAILED DESCRIPTION - A detailed description of the configuration of the BRD are required.

BRD DIAGRAM - A detailed diagram of the BRD (B-4) used is required to be provided. Photographs of the BRD are required to be provided.

GEAR DIAGRAM - A detailed diagram of the BRD configuration including placement and measurements (e.g., number of meshes) of all trawl components including the BRD and TED used is required to be provided.

The NMFS requires this collection of information to minimize the bycatch of finfish in the southeastern shrimp fishery. The data and testing will be used to develop improved bycatch reduction devices (BRDs). Responses are required under the Magnuson-Stevens Act to obtain certification that allows use of a BRD in the shrimp fishery of the Gulf of Mexico. Data will be confidential pursuant to the Magnuson-Stevens Act and other applicable law. Notwithstanding any other provisions of the law, no person is required to, nor shall any person be subject to a penalty to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Southeast Regional Office, National Marine Fisheries Service, 263 13th Avenue South, St. Petersburg, FL 33701.

APPENDIX D OMB No. 0648 -0345 Approval Expires - 06/30/2008

STATION SHEET BRD EVALUATION
BRD TESTING PROTOCOL

ORG PRO | TRIP NO. | VESSEL | TOW NO. | OBSERVER | MONTH DAY YEAR DATE

TIME IN | DEGREE MINUTE SECONDS LATITUDE IN | DEGREE MINUTE SECONDS LONGITUDE IN | DEPTH IN (FEET)

TIME OUT | DEGREE MINUTE SECONDS LATITUDE OUT | DEGREE MINUTE SECONDS LONGITUDE OUT | DEPTH OUT (FEET)

HOURS TOWED | KNOTS VESSEL SPEED | STAT ZONE | 1 2 3 4 OPERATION CODE | TOTAL NETS | SEA STATE

NET POSITION SAMPLED | BRD OPEN (E) BRD CLOSED (C) | SAMPLE WEIGHT (kg) *of one-basket characterization sample; if done.*

TOTAL CATCH WEIGHT (kg) | SHRIMP TOTAL WEIGHT (kg) | SHRIMP - OR | HEAD ON (O) HEAD OFF (X)

FINFISH TOTAL WEIGHT (kg)

Attach length frequency form for red snapper

RED SNAPPER TOTAL WEIGHT (kg) | RED SNAPPER TOTAL NUMBER | NO. OF RED SNAPPER LESS THAN OR EQUAL TO 100 mm | NO. OF RED SNAPPER GREATER THAN 100 mm

Comments:

NET POSITION SAMPLED | BRD OPEN (E) BRD CLOSED (C) | SAMPLE WEIGHT (kg) *of one-basket characterization sample; if done.*

TOTAL CATCH WEIGHT (kg) | SHRIMP TOTAL WEIGHT (kg) | SHRIMP - OR | HEAD ON (O) HEAD OFF (X)

FINFISH TOTAL WEIGHT (kg)

Attach length frequency form for red snapper

RED SNAPPER TOTAL WEIGHT (kg) | RED SNAPPER TOTAL NUMBER | NO. OF RED SNAPPER LESS THAN OR EQUAL TO 100 mm | NO. OF RED SNAPPER GREATER THAN 100 mm

Comments:

Characterization (one basket) for each net ☐ YES (Attach Species Forms) ☐ NO

Captain's Signature

INSTRUCTIONS FOR THE STATION SHEET

This form is split into two sections, the first part is for location information and the second part is for sample information. For both sections, 999's should be entered as a default code for all numeric fields where data are not available, with an explanation given in the comments section. The sample section is divided, half is for the first net being sampled, and the other half is for the second net sampled.

SECTION 1

TRIP NO: Transcribe the Vessel Information Form.

VESSEL: Transcribe the Vessel Information Form.

TOW NUMBER: Enter the appropriate tow number. The tow number starts at 001 for each trip.

OBSERVER: Enter the observers (your) initials, first, middle, and last.

DATE: Using two digits for month, day, and year (MO/DY/YR) enter the appropriate information (e.g., 6 May 1998 is 050698).

TIME IN: Enter the time that the nets are set (i.e., "dog off" time). Use military time, midnight is 0000, 1 A.M. is 0100, 1 P.M. is 1300. Military time uses a 24 hour clock for time keeping.

LATITUDE IN: Enter the position of the vessel at the tow start time in degrees, minutes and seconds. ASK THE CAPTAIN IF THE LORAN or GPS UNIT READS IN DEGREES, MINUTES, AND SECONDS OR IN DEGREES, MINUTES, AND HUNDREDTHS OF A MINUTE. If the unit reads in hundredths of minutes, multiply the last two digits (as a decimal figure) by 60 to obtain the seconds (e.g., .33 X 60 = 19.8 seconds this is rounded up to 20 seconds).

LONGITUDE IN: Enter the position of the vessel at the tow start time in degrees, minutes and seconds. Remember to correct the data if necessary.

DEPTH IN (IN FEET): Enter the water depth at the start of the tow. ASK THE CAPTAIN IF THE TRANSPONDER IS MOUNTED AT THE WATER LINE OR ON THE KEEL. IF THE WATER DEPTH IS MEASURED FROM ANYWHERE BUT THE WATER LINE THEN ADD THE DEPTH OF THE TRANSPONDER TO THE DEPTH READING.

TIME OUT: Enter the time at the start of haul back.

LATITUDE OUT: Enter the position of the vessel at the start of haul back in degrees, minutes and seconds. Remember to correct the data if necessary.

LONGITUDE OUT: Enter the position of the vessel at the start of haul back in degrees, minutes and seconds. Remember to correct the data if necessary.

DEPTH OUT: (IN FEET) - Enter the water depth at the end of the tow. Remember to correct the data for true depth if necessary.

HOURS TOWED: COMPUTE THE HOURS TOWED FROM TIME IN TO THE TIME OUT. Enter this information in hours and tenths of hours (e.g., one hour and thirty minutes is 1.5 hours).

VESSEL SPEED: This information comes from the Captain and should be in KNOTS.

STAT ZONE: Enter the appropriate statistical zone **(at time in)** for Gulf of Mexico or southeastern Atlantic. Leave blank if towing is done outside the statistical zones, and explain in comments.

OPERATIONAL CODE: Select the appropriate operational code for each net. Generally, a successful tow is denoted as ZZYZ, with Z being a successful trawl for a net position, and Y indicating that a "Try Net" was towed in front of net # 3. See the operational codes listing for the appropriate code for your situation. In situations were several problems affect a tow, generally the most severe problem is recorded. If the nets are bogged down due to mud, the operational code would read BBBB. For unsuccessful tows (other than ZZYZ) please give further explanation in the comments section.

TOTAL NETS: Enter the total number of nets trawled (e.g., 2 or 4). Do not include the try net in this count.

SEA STATE: Sea state is measured as wave height in feet. Enter the number that best describes the sea state: 1 = 0-2 feet, 2 = 3-5 feet, 3 = 6-8 feet, 4 = 8+ feet

SECTION 2

NET POSITION SAMPLED: Enter the net position number of the sample net. PORT AND STARBOARD ARE DETERMINED BY FACING THE BOW OF THE VESSEL WHILE ON THE STERN, STARBOARD IN ON THE RIGHT AND PORT IS ON THE LEFT. (Net # 1 is the outside port net and is usually the first recorded on the form).

BRD OPEN (E) or BRD CLOSED (C): Enter "E" if net is experimental and has BRD typically opened or "C" if net is the "Control" and the BRD is typically closed.

SAMPLE WEIGHT: After mixing the catch, obtain a one basket sample (approximately 70 pounds) from each the control and experimental nets. Then remove all target fish species (e.g., red snapper) and weigh the basket. Enter the weight in kilograms. If either the experimental net or the control net has an operational code of other than "Z", enter 99.9 as a default code denoting that a sample was not taken.

TOTAL CATCH WEIGHT: Enter the weight of the total catch (in kilograms) from the net.

SHRIMP TOTAL WEIGHT: Enter the weight of all penaeid (brown, white, pink) shrimp. Remember to add in the weight of penaeid shrimp from the characterization sample.

SHRIMP - HEAD ON OR HEAD OFF: Enter "O" if the head is left on the shrimp or "X" if the head is removed.

FINFISH TOTAL CATCH WEIGHT: Enter the weight of the total finfish catch (in kilograms) from the net, or if sampled, the total finfish catch in the sample.

RED SNAPPER TOTAL WEIGHT: Enter the total weight in kilograms of all red snapper.

RED SNAPPER TOTAL NUMBER: Enter the total number of red snapper.

NO. OF RED SNAPPER LESS THAN OR EQUAL TO 100 mm: Enter the total number of red snapper that have a fork length of less than 100 mm. (Attach the length frequency form for red snapper).

NO. OF RED SNAPPER GREATER THAN 100 mm: Enter the total number of red snapper that have a fork length greater than 100 mm. (Attach the length frequency form for red snapper).

COMMENTS: Enter any appropriate information to the trawl (e.g., nets bogged down with mud, net torn, tire blocking TED).

CAPTAIN'S SIGNATURE: At the Captain's convenience, have him sign this form. This is to verify that the data were collected.

The NMFS requires this collection of information to minimize the bycatch of finfish in the southeastern shrimp fishery. The data and testing will be used to develop improved bycatch reduction devices (BRDs). Responses are required under the Magnuson-Stevens Act to obtain certification that allows use of a BRD in the shrimp fishery of the Gulf of Mexico. Data will be confidential pursuant to the Magnuson-Stevens Act and other applicable law. Notwithstanding any other provisions of the law, no person is required to, nor shall any person be subject to a penalty to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Southeast Regional Office, National Marine Fisheries Service, 263 13th Avenue South, St. Petersburg, FL 33701.

OPERATION CODES

A = Nets not spread; typically doors are flipped or doors hung together so net could not spread.

B = Gear bogged; the net has picked up a quantity of sand or mud such that the net can not be easily towed.

C = Bag choked; the catch in the net is prevented from getting into the bag by something (grass, sticks, turtle, etc.) clogging net or by the twisting of the lazy-line.

D = Gear not digging; the net is fishing off the bottom due to insufficient weight.

E = Twisted warp or line; the cables composing the bridle get twisted (from passing over blocks which occasionally must be removed before continuing to fish). Use this code if catch was affected.

F = Gear fouled; the gear has become entangled in itself. Typically this involves the webbing and some object like a float or chains.

G = Bag untied; bag of net not tied when dragging net.

H = Rough weather; if the weather is so bad fishing is stopped, then the previous tow should receive this code if the rough conditions affected the catch.

I = Torn webbing or lost net; usually results from hanging the net and tearing it loose. The net comes back with large tears if at all. Do not use this code if there are only a few broken meshes. Continue using this code until net is repaired or replaced.

J = Dumped catch; tow was made but catch was discarded, perhaps because of too much trash, fish, sponge. Give reason in Comments.

K = No pick up; tow made but net not dumped on deck because nets are brought up, boat changes location and nets are towed more before decking.

L = Hung up; untimely termination of a tow by a hang. Specify trawl(s) which were hung and caused lost time in Comments.

M = Bags dumped together and catches not separated.

N = Net did not fish; no apparent cause.

O = Gear fouled on object. Net may be towed but performance is affected. Give specifics in Comments.

P = No measurement taken of shrimp or total catch.

Q = Cable breaks and net lost. Describe in Comments.

R = Net caught in wheel.

S = Tickler chain fouled or tangled.

T = Other problems.

U = Excluder gear disabled.

W = Defective excluder gear.

Y = Net trailing behind try net.

Z = Successful tow.

Factors Affecting Shrimp Retention

High Shrimp Retention - Fish Eyes

1. Fast towing speed (2.8 - 3.0 knots).
2. Fast winch retrieval speed.
3. 120 meshes or greater bag.
4. Minimal /no turning.
5. Minimal tides.
6. Minimal debris.
7. Fair weather.

Reduced Shrimp Retention - Fish Eyes

1. Reduced/restricted tow speed <2.3 knots.
2. Slow winch retrieval.
3. Small bags 80-100 meshes.
4. Excessive turning.
5. Strong tides.
6. Debris, crab traps and jellyfish.
7. Rough weather.

Source: Georgia Marine Extension Service, 1997.

OMB No. 648-0345 Approval Expires- 06/30/2008

APPENDIX E

LENGTH FREQUENCY FORM (TARGET SPECIES)
BRD TESTING PROTOCOL

ORG PRO

TRIP NO.

VESSEL

TOW NUMBER

NET POSITION

Control (C) or Experimental (E)

GENUS	GENUS	GENUS
SPECIES MEAS.CODE	SPECIES MEAS.CODE	SPECIES MEAS.CODE

	LENGTH (MM)		LENGTH (MM)		LENGTH (MM)
1		1		1	
2		2		2	
3		3		3	
4		4		4	
5		5		5	
6		6		6	
7		7		7	
8		8		8	
9		9		9	
10		10		10	
11		11		11	
12		12		12	
13		13		13	
14		14		14	
15		15		15	
16		16		16	
17		17		17	
18		18		18	
19		19		19	
20		20		20	
21		21		21	
22		22		22	
23		23		23	
24		24		24	
25		25		25	
26		26		26	
27		27		27	
28		28		28	
29		29		29	
30		30		30	

REVISED 08/31/98

INSTRUCTIONS FOR
LENGTH FREQUENCY FORM
BRD TESTING PROTOCOL

The length frequency forms are provided for convenience should the applicant choose to take lengths on certain species taken in the bycatch, such as red snapper or weakfish. The applicant may need to use more than one column for a species depending the number contained in your net.

TRIP NO: Transcribe from Station Sheet.

VESSEL: Transcribe from Station Sheet.

TOW NO.: Transcribe from Station Sheet.

NET POSITION: Transcribe from Station Sheet.

GENUS-SPECIES: Enter the first seven characters of the genus and the first six characters of the species name. If not identified to species, continue genus name into species block if longer than seven characters. Use family name if specimen can not be identified to species. The highlighted last two squares are for the measurement code which indicates the measurement utilized. For red snapper, Spanish mackerel and king mackerel the measurement code is 01 (measure fork length).

L	U	T	J	A	N	U	
C	A	M	P	E	C	0	1

MEASUREMENT CODE:

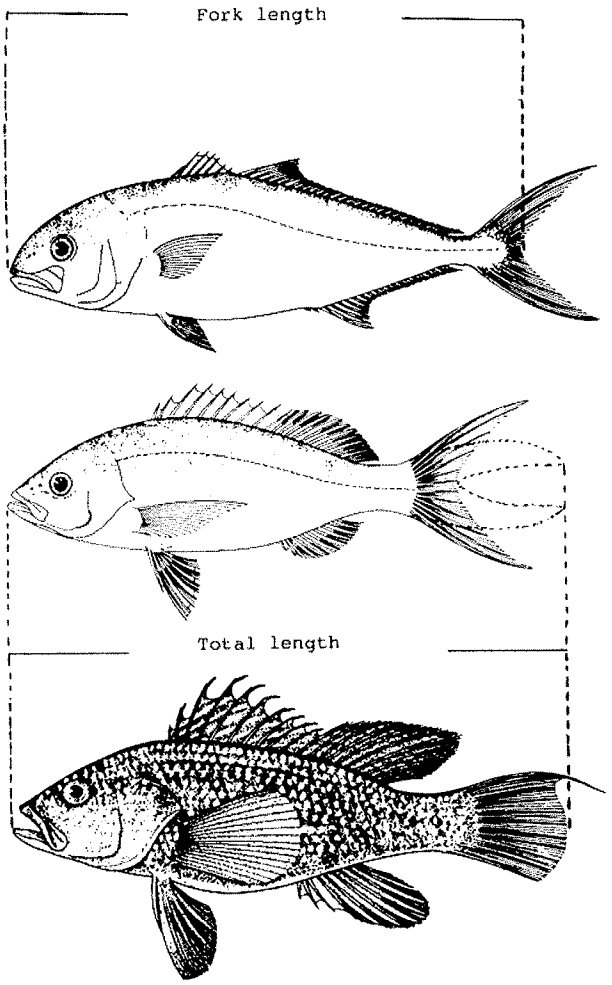
Step # 1: Identify the sample species.

Step # 2: Measure the organism (in millimeters) and record the measurement on the sheet.

The NMFS requires this collection of information to minimize the bycatch of finfish in the southeastern shrimp fishery. The data and testing will be used to develop improved bycatch reduction devices (BRDs). Responses are required under the Magnuson-Stevens Act to obtain certification that allows use of a BRD in the shrimp fishery of the Gulf of Mexico. Data will be confidential pursuant to the Magnuson-Stevens Act and other applicable law. Notwithstanding any other provisions of the law, no person is required to, nor shall any person be subject to a penalty to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Southeast Regional Office, National Marine Fisheries Service, 263 13th Avenue South, St. Petersburg, FL 33701.

Illustration of fork Length and Total Length Measurement



OMB No. 0648-0345 Approval Expires - 06/30/2008

APPENDIX F

SPECIES CHARACTERIZATION FORM
BRD TESTING PROTOCOL

Trip No.	Vessel	Tow No.	Net Position	Control (C) Experimental (E)

COMMON NAME	GENUS	SPECIES	YOY X	NUMBER	SAMPLE WEIGHT(kg)	SELECT WEIGHT (kg)
CRABS, LOBSTERS, ETC.	CRUSTAC			1	.	.
OTHER INVERTEBRATES	INVERTE			1	.	.
SHARKS (ALL SPECIES)	CARCHAR				.	.
TROUT	CYNOSCI				.	.
SNAPPER (OTHER)	LUTJANU				.	.
LANE SNAPPER	LUTJANU	SYNAGR			.	.
CROAKER	MICROPO	UNDULA			.	.
SOUTHERN FLOUNDER	PARALIC	LETHOS			.	.
BLACK DRUM	POGONIA	CROMIS			.	.
COBIA	RACHYCE	CANADU			.	.
VERMILION SNAPPER	RHOMBOP	AURORU			.	.
RED DRUM	SCIAENO	OCELLA			.	.
SPOTTED SEATROUT	CYNOSCI	NEBULO			.	.
KING MACKEREL	SCOMBER	CAVALL			.	.
SPANISH MACKEREL	SCOMBER	MACULA			.	.
LONGSPINE PORGY	STENOTO	CAPRIN			.	.
OTHER FINFISH-GROUPED	PISCES			1	.	.
DEBRIS	DEBRIS			1	.	.

OTHER NOT LISTED						
					.	.
					.	.
					.	.

FOR ATLANTIC						
WEAKFISH (GRAY TROUT)	CYNOSCI	REGALI			.	.

REVISED 08/21/00

INSTRUCTIONS FOR THE SPECIES CHARACTERIZATION FORM BRD TESTING PROTOCOL

TRIP NO.: Enter the trip number. The organization will provide this information to the observer prior to their departure from port.

VESSEL: Enter the vessel code.

TOW NUMBER: Enter the appropriate tow number.

NET POSITION: Enter the net position sample was taken from.

CONTROL (C) OR EXPERIMENTAL (E): Enter the appropriate code for this the sample net.

Procedure.

After obtaining a total weight for each the control and experimental nets, keep one basket (approximately 70 pounds) from each of the nets for species characterization (i.e., one basket from control net and one basket from the experimental net). Weigh the basket to obtain a sample weight which is entered on the station sheet (Remember to enter 9's for sample weight if a characterization is not done).

Processing the Catch

Become familiar with the species listed on this form. These organisms will be grouped by species, counted and weighed. All other organisms will be separated into the following categories:

1) Crabs, Lobster, etc. (Crustacea): includes shrimp other than brown, white, and pink shrimp. Mantis shrimp, sugar shrimp, seabobs, crabs, lobsters, etc. would be included in this group as well.

2) Other Invertebrates: includes organisms like squid, jelly fish, starfish, sea pansies, shells, etc.

3) Other Finfish (Pisces): includes all other fish, skates and rays not listed on the pre-printed station sheet. If the dominant fish species in your sample is not listed on the pre-printed station sheet, enter the common and scientific name, count and weight for that species group on the pre-printed list.

4) Debris: Includes miscellaneous debris such as chunks of mud, rocks, sticks, etc.

A group weight should be obtained for each of these four categories and entered this form. You do not have to count each organism within a category, a default code of 1 has already been entered in the number column.

1) Brown, White, and Pink Shrimp: All penaeid shrimp should be removed from the sample first. Separate by species, count, and weigh. The weights of these shrimp have to be added to the total

weight for all shrimp from the sampled net. If the boat is heading their shrimp, then these shrimp have to weighed without heads before adding the weight to the total shrimp weight.

2) Fish: Sharks - use this category for all species of sharks; Trout - this includes all species of sea trout except spotted seatrout; Snapper (Other) - remember, this category is for "Lutjanus" species only. This does not include wenchman snappers; Lane snapper - commonly referred to as a "candy snapper"; Whiting - this category is for all species of whiting; Croaker - sometimes confused with the spot which has a conspicuous spot just above the pectoral fin; Southern Flounder - be careful not to confuse this species with other common flatfish found in the trawls; Black Drum - juveniles sometimes confused with sheepshead; Cobia - Juveniles sometimes confused with sharksuckers; Vermilion Snapper - easily confused with wenchman snapper which are usually more common offshore; Red Drum; Spotted Seatrout; King Mackerel - deep posterior downward slope to lateral line; Spanish Mackerel - Shallow posterior slope to lateral line; Longspine Porgy - very common on offshore shrimp grounds.

Select Species

If a particular species is to be selected out of the total catch, and not just the sample, record the species group weight in the select weight column. Generally this occurs when the species is of commercial importance (i.e., mackerels) or rare. The project manager will inform you prior to the trip what commercial species (if any) are select. If a species is rare (i.e., not generally trawl caught) select that species out of the entire catch of the net selected for sampling. If the catch was worked up in its entirety (i.e., less than one basket), all entries will be in the select column.

OMB No. 648-0345 Approval Expires- 06/30/2008

APPENDIX G

CONDITION AND FATE FORM
BRD TESTING PROTOCOL

CONTROL NET | NET POSITION ☐

CONDITION AND FATE OF BYCATCH PRIOR TO DISCARDING

FISH

- ☐ MORE THAN 50% OF CATCH ALIVE
- ☐ MORE THAN 50% OF CATCH DEAD
- ☐ NOT DETERMINED
- ☐ NOT OBSERVED

COMMENTS: _____

INVERTEBRATES

- ☐ MORE THAN 50% OF CATCH ALIVE
- ☐ MORE THAN 50% OF CATCH DEAD
- ☐ NOT DETERMINED
- ☐ NOT OBSERVED

COMMENTS: _____

PREDATORS OBSERVED

- ☐ SHARKS
- ☐ DOLPHINS
- ☐ SEA BIRDS
- ☐ OTHER FISH
- ☐ NONE
- ☐ NOT OBSERVED

COMMENTS: _____

(ESTIMATED # OF ORGANISMS) SEEN EXITING BRD DURING NET RETRIEVAL

- ☐ (1 - 10)
- ☐ (10 - 50)
- ☐ (50 - 100)
- ☐ (100 OR MORE)
- ☐ NONE
- ☐ N/A (BRD closed)
- ☐ NOT OBSERVED (or not able to see.)

COMMENTS: _____

PREDATORS ACTIVELY FEEDING ON ORGANISMS ESCAPING FROM BRD OPENING? (CHECK ONE)

☐ Yes ☐ No ☐ Not Observed (or not able to see.)

List predator types: _____

EXPERIMENTAL NET | NET POSITION ☐

CONDITION AND FATE OF BYCATCH PRIOR TO DISCARDING

FISH

- ☐ MORE THAN 50% OF CATCH ALIVE
- ☐ MORE THAN 50% OF CATCH DEAD
- ☐ NOT DETERMINED
- ☐ NOT OBSERVED

COMMENTS: _____

INVERTEBRATES

- ☐ MORE THAN 50% OF CATCH ALIVE
- ☐ MORE THAN 50% OF CATCH DEAD
- ☐ NOT DETERMINED
- ☐ NOT OBSERVED

COMMENTS: _____

PREDATORS OBSERVED

- ☐ SHARKS
- ☐ DOLPHINS
- ☐ SEA BIRDS
- ☐ OTHER FISH
- ☐ NONE
- ☐ NOT OBSERVED

COMMENTS: _____

(ESTIMATED # OF ORGANISMS) SEEN EXITING BRD DURING NET RETRIEVAL

- ☐ (1 - 10)
- ☐ (10 - 50)
- ☐ (50 - 100)
- ☐ (100 OR MORE)
- ☐ NONE
- ☐ N/A (BRD closed)
- ☐ NOT OBSERVED (or not able to see.)

COMMENTS: _____

PREDATORS ACTIVELY FEEDING ON ORGANISMS ESCAPING FROM BRD OPENING? (CHECK ONE)

☐ Yes ☐ No ☐ Not Observed (or not able to see.)

List predator types: _____

Revised 08/31/99

INSTRUCTIONS FOR THE CONDITION & FATE FORM BRD TESTING PROTOCOL

TRIP NUMBER: Transcribe this information from the Vessel Information form.

VESSEL: Transcribe this code information from the Vessel Information form.

TOW NUMBER: Enter the appropriate tow number. The Tow Number starts at 001 for each trip. Remember, tows not sampled do not receive a tow number.

THIS FORM IS USED FOR BOTH NETS; LEFT SIDE FOR THE CONTROL NET AND THE RIGHT SIDE FOR THE EXPERIMENTAL NET.

CONTROL NET (BRD CLOSED)

NET POSITION CONTROL NET (BRD CLOSED): Enter the net position number of the net which has the BRD closed.

CONDITION AND FATE OF BYCATCH PRIOR TO DISCARDING

FISH: Select and mark one of the four categories listed

INVERTEBRATES: Select and mark one of the four categories listed. In the comments block enter any appropriate information.

PREDATORS OBSERVED: Select and mark the appropriate category. In the comments block enter any appropriate information.

EXPERIMENTAL NET (BRD OPEN)

NET POSITION EXPERIMENTAL NET (BRD OPEN): Enter the net position number of the net which has the BRD open.

CONDITION AND FATE OF BYCATCH PRIOR TO DISCARDING

FISH: Select and mark one of the four categories listed

INVERTEBRATES: Select and mark one of the four categories listed. In the comments block enter any appropriate information.

PREDATORS OBSERVED: Select and mark the appropriate category. In the comments block enter any appropriate information.

ESTIMATED # OF ORGANISMS SEEN EXITING BRD DURING NET RETRIEVAL: Select and mark the appropriate category. In the comments block list any predator(s) seen feeding on escaping organisms. The predator(s) may be feeding at the BRD opening or anywhere along the net following the escaping organisms.

The NMFS requires this collection of information to minimize the bycatch of finfish in the southeastern shrimp fishery. The data and testing will be used to develop improved bycatch reduction devices (BRDs). Responses are required under the Magnuson-Stevens Act to obtain certification that allows use of a BRD in the shrimp fishery of the Gulf of Mexico. Data will be confidential pursuant to the Magnuson-Stevens Act and other applicable law. Notwithstanding any other provisions of the law, no person is required to, nor shall any person be subject to a penalty to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Southeast Regional Office, National Marine Fisheries Service, 263 13th Avenue South, St. Petersburg, FL 33701.

INSTRUCTIONS FOR THE VESSEL INFORMATION FORM

APPENDIX H

QUALIFICATIONS OF OBSERVER

To be qualified as an observer operating under this Protocol, an individual must have a Bachelor's degree in fisheries biology or closely related field from an accredited college, have at least 6 months experience working with a university, college, state fisheries agency, NMFS, or private research organization such as the Gulf and South Atlantic Fisheries Foundation, Inc., as an observer on a trawler (including research trawlers) in the southeast region, or have successfully completed a training course conducted or approved by the Director of the NMFS Southeast Fisheries Science Center. A list of qualified observers is maintained by the RA.

An individual wishing to be included on the list of qualified observers, but who is not directly involved in any current bycatch observer programs, should submit a resume and supporting documents to the Director, Southeast Fisheries Science Center, 75 Virginia Beach Drive, Miami, FL 33149. Supporting information must include the names, addresses, and telephone numbers of at least three references who can attest to the applicant's background, experiences, and professional ability. These references will be contacted; unsatisfactory references may be a basis for disapproval of an applicant as an observer. The Center will use this information to determine which names will to be included on a list of qualified observers. If an applicant is not approved as an observer, the RA will notify the applicant of the disapproval and will provide an explanation for the denial.

APPENDIX I

OMB NUMBER 0648-0345 OMB APPROVAL EXPIRES - 06/30/2008

VESSEL INFORMATION FORM
BRD TESTING PROTOCOL

___ ___ ___ ___ ___ ___ ___ ___ ___

Trip. No. Vessel

DATE (MO/DY/YR): _____

OBSERVER NAME: _____

VESSEL NAME: _____

VESSEL LENGTH (ft.) _____

VESSEL IDENTIFICATION NUMBER: _____

YEAR VESSEL BUILT: _____

VESSEL TYPE (CIRCLE ONE): FREEZER OR ICE BOAT

MATERIAL OF HULL CONSTRUCTION (CIRCLE ONE):

STEEL WOOD FIBERGLASS

GROSS TONNAGE: _____

HORSEPOWER OF ENGINE: _____

CREW SIZE (WITHOUT CAPTAIN): _____

OWNER NAME: _____

OWNER ADDRESS: _____

CAPTAIN'S NAME: _____

OWNER'S OR CAPTAINS SIGNATURE: _____

POSITION, IF OWNER IS
A CORPORATION OR PARTNER: _____

TRIP NO. The trip number will be assigned to you prior to departure. The trip number is designated by the organization (e.g., NMFS, Foundation, BRD certification applicant). The trip number consists of five characters:

The first character refers to the organization conducting the project.

G = NMFS, Galveston Laboratory
F = Foundation, Gulf of Mexico
S = Foundation, South Atlantic
T = Texas Shrimp Association
D = Georgia DNR
N = North Carolina Sea Grant/State Resource Agency

The second character refers to the project type.

B = BRD Evaluation
C = Bycatch Characterization
G = BRD Certification, Gulf of Mexico
M = Modified Bycatch Characterization
N = Naked Net (TED alternative)
R = Red Snapper Initiative
S = BRD Certification, South Atlantic
T = TED Evaluation
X = Rock Shrimp Characterization
Z = Soft TED Evaluation

The third through fifth characters identify the number of the trip.

VESSEL: Enter the vessel code. This will be provided to you prior to departure. This is typically the initials of the vessel (e.g., Miss Kelly - MKE). If a duplication should occur (i.e., more than one vessel having the same two letter code), the organization will assign the vessel another code. For repeat trips on the same vessel, the same vessel code should be used

DATE (MO/DY/YR): Enter month, day, and year.

OBSERVER NAME: Print full name of the qualified observer conducting the test.

VESSEL NAME: Write the vessel's full name.

VESSEL LENGTH (ft.): Enter the vessel's overall length (feet). Get this information from the Captain.

VESSEL IDENTIFICATION NUMBER: Enter State or Federal vessel registration number.

YEAR VESSEL BUILT: Self-explanatory.

VESSEL TYPE (CIRCLE ONE): FREEZER OR ICE BOAT Self-explanatory.

MATERIAL OF HULL CONSTRUCTION (CIRCLE ONE):
STEEL WOOD FIBERGLASS Self-explanatory.

GROSS TONNAGE: Get this information from the Captain.

HORSEPOWER OF ENGINE: Get this information from the Captain.

CREW SIZE (WITHOUT CAPTAIN): Self-explanatory.

OWNER NAME: Self-explanatory.

OWNER ADDRESS: Self-explanatory.

CAPTAIN'S NAME: Self-explanatory.

OWNER'S OR CAPTAIN'S SIGNATURE: Self-explanatory.

POSITION, IF OWNER IS A CORPORATION OR PARTNERSHIP: Self-explanatory.

The NMFS requires this collection of information to minimize the bycatch of finfish in the southeastern shrimp fishery. The data and testing will be used to develop improved bycatch reduction devices (BRDs). Responses are required under the Magnuson-Stevens Act to obtain certification that allows use of a BRD in the shrimp fishery of the Gulf of Mexico. Data will be confidential pursuant to the Magnuson-Stevens Act and other applicable law. Notwithstanding any other provisions of the law, no person is required to, nor shall any person be subject to a penalty to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Public reporting burden for this collection of information is estimated to average 20 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Southeast Regional Office, National Marine Fisheries Service, 263 13th Avenue South, St. Petersburg, FL 33701.

SEC. 303. CONTENTS OF FISHERY MANAGEMENT PLANS 16 U.S.C. 1853

95-354, 99-659, 101-627, 104-297

(a) REQUIRED PROVISIONS.—Any fishery management plan which is prepared by any Council, or by the Secretary, with respect to any fishery, shall—

(1) contain the conservation and management measures, applicable to foreign fishing and fishing by vessels of the United States, which are—

(A) necessary and appropriate for the conservation and management of the fishery to prevent overfishing and rebuild overfished stocks, and to protect, restore, and promote the long-term health and stability of the fishery;

(B) described in this subsection or subsection (b), or both; and

(C) consistent with the national standards, the other provisions of this Act, regulations implementing recommendations by international organizations in which the United States participates (including but not limited to closed areas, quotas, and size limits), and any other applicable law;

(2) contain a description of the fishery, including, but not limited to, the number of vessels involved, the type and quantity of fishing gear used, the species of fish involved and their location, the cost likely to be incurred in management, actual and potential revenues from the fishery, any recreational interest in the fishery, and the nature and extent of foreign fishing and Indian treaty fishing rights, if any;

(3) assess and specify the present and probable future condition of, and the maximum sustainable yield and optimum yield from, the fishery, and include a summary of the information utilized in making such specification;

(4) assess and specify—

(A) the capacity and the extent to which fishing vessels of the United States, on an annual basis, will harvest the optimum yield specified under paragraph (3),

(B) the portion of such optimum yield which, on an annual basis, will not be harvested by fishing vessels of the United States and can be made available for foreign fishing, and

(C) the capacity and extent to which United States fish processors, on an annual basis, will process that portion of such optimum yield that will be harvested by fishing vessels of the United States;

109-479

(5) specify the pertinent data which shall be submitted to the Secretary with respect to commercial, recreational, charter fishing, and fish processing in the fishery, including, but not limited to, information regarding the type and quantity of fishing gear used, catch by species in numbers of fish or weight thereof, areas in which fishing was engaged in, time of fishing, number of hauls, economic information necessary to meet the requirements of this Act, and the estimated processing capacity of, and the actual processing capacity utilized by, United States fish processors;

(6) consider and provide for temporary adjustments, after consultation with the Coast Guard and persons utilizing the fishery, regarding access to the fishery for vessels otherwise prevented from harvesting because of weather or other ocean conditions affecting the safe conduct of the fishery; except that the adjustment shall not adversely affect conservation efforts in other fisheries or discriminate among participants in the affected fishery;

(7) describe and identify essential fish habitat for the fishery based on the guidelines established by the Secretary under section 305(b)(1)(A), minimize to the extent practicable adverse effects on such habitat caused by fishing, and identify other actions to encourage the conservation and enhancement of such habitat;

(8) in the case of a fishery management plan that, after January 1, 1991, is submitted to the Secretary for review under section 304(a) (including any plan for which an amendment is submitted to the Secretary for such review) or is prepared by the Secretary, assess and specify the nature and extent of scientific data which is needed for effective implementation of the plan;

109-479

(9) include a fishery impact statement for the plan or amendment (in the case of a plan or amendment thereto submitted to or prepared by the Secretary after October 1, 1990) which shall assess, specify, and analyze the likely effects, if any, including the cumulative conservation, economic, and social impacts, of the conservation and management measures on, and possible mitigation measures for—

(A) participants in the fisheries and fishing communities affected by the plan or amendment;

(B) participants in the fisheries conducted in adjacent areas under the authority of another Council, after consultation with such Council and representatives of those participants; and

(C) the safety of human life at sea, including whether and to what extent such measures may affect the safety of participants in the fishery;

(10) specify objective and measurable criteria for identifying when the fishery to which the plan applies is overfished (with an analysis of how the criteria were determined and the relationship of the criteria to the reproductive potential of stocks of fish in that fishery) and, in the case of a fishery which the Council or the Secretary has determined is approaching an overfished condition or is overfished, contain conservation and management measures to prevent overfishing or end overfishing and rebuild the fishery;

(11) establish a standardized reporting methodology to assess the amount and type of bycatch occurring in the fishery, and include conservation and management measures that, to the extent practicable and in the following priority—

(A) minimize bycatch; and

(B) minimize the mortality of bycatch which cannot be avoided;

(12) assess the type and amount of fish caught and released alive during recreational fishing under catch and release fishery management programs and the mortality of such fish, and include conservation and management measures that, to the extent practicable, minimize mortality and ensure the extended survival of such fish;

109-479

(13) include a description of the commercial, recreational, and charter fishing sectors which participate in the fishery, including its economic impact, and, to the extent practicable, quantify trends in landings of the managed fishery resource by the commercial, recreational, and charter fishing sectors;

109-479

(14) to the extent that rebuilding plans or other conservation and management measures which reduce the overall harvest in a fishery are necessary, allocate, taking into consideration the economic impact of the harvest restrictions or recovery benefits on the fishery participants in each sector, any harvest restrictions or recovery benefits fairly and equitably among the commercial, recreational, and charter fishing sectors in the fishery and;

109-479

(15) establish a mechanism for specifying annual catch limits in the plan (including a multiyear plan), implementing regulations, or annual specifications, at a level such that overfishing does not occur in the fishery, including measures to ensure accountability.

97-453, 99-659, 101-627, 102-251, **104-297**

(b) DISCRETIONARY PROVISIONS.—Any fishery management plan which is prepared by any Council, or by the Secretary, with respect to any fishery, may—

(1) require a permit to be obtained from, and fees to be paid to, the Secretary, with respect to—

(A) any fishing vessel of the United States fishing, or wishing to fish, in the exclusive economic zone [or special areas,]* or for anadromous species or Continental Shelf fishery resources beyond such zone [or areas]*;

(B) the operator of any such vessel; or

(C) any United States fish processor who first receives fish that are subject to the plan;

109-479

(2)(A) designate zones where, and periods when, fishing shall be limited, or shall not be permitted, or shall be permitted only by specified types of fishing vessels or with specified types and quantities of fishing gear;

(B) designate such zones in areas where deep sea corals are identified under section 408, to protect deep sea corals from physical damage from fishing gear or to prevent loss or damage to such fishing gear from interactions with deep sea corals, after considering long-term sustainable uses of fishery resources in such areas; and

(C) with respect to any closure of an area under this Act that prohibits all fishing, ensure that such closure—

(i) is based on the best scientific information available;

(ii) includes criteria to assess the conservation benefit of the closed area;

(iii) establishes a timetable for review of the closed area's performance that is consistent with the purposes of the closed area; and

(iv) is based on an assessment of the benefits and impacts of the closure, including its size, in relation to other management measures (either alone or in combination with such measures), including the benefits and impacts of limiting access to: users of the area, overall fishing activity, fishery science, and fishery and marine conservation;

(3) establish specified limitations which are necessary and appropriate for the conservation and management of the fishery on the—

(A) catch of fish (based on area, species, size, number, weight, sex, bycatch, total biomass, or other factors);

(B) sale of fish caught during commercial, recreational, or charter fishing, consistent with any applicable Federal and State safety and quality requirements; and

(C) transshipment or transportation of fish or fish products under permits issued pursuant to section 204;

(4) prohibit, limit, condition, or require the use of specified types and quantities of fishing gear, fishing vessels, or equipment for such vessels, including devices which may be required to facilitate enforcement of the provisions of this Act;

109-479

(5) incorporate (consistent with the national standards, the other provisions of this Act, and any other applicable law) the relevant fishery conservation and management measures of the coastal States nearest to the fishery and take into account the different circumstances affecting fisheries from different States and ports, including distances to fishing grounds and proximity to time and area closures;

109-479

(6) establish a limited access system for the fishery in order to achieve optimum yield if, in developing such system, the Council and the Secretary take into account—

(A) present participation in the fishery;

(B) historical fishing practices in, and dependence on, the fishery;

(C) the economics of the fishery;

(D) the capability of fishing vessels used in the fishery to engage in other fisheries;

(E) the cultural and social framework relevant to the fishery and any affected fishing communities;

(F) the fair and equitable distribution of access privileges in the fishery; and

(G) any other relevant considerations;

(7) require fish processors who first receive fish that are subject to the plan to submit data which are necessary for the conservation and management of the fishery;

(8) require that one or more observers be carried on board a vessel of the United States engaged in fishing for species that are subject to the plan, for the purpose of collecting data necessary for the conservation and management of the fishery; except that such a vessel shall not be required to carry an observer on board if the facilities of the vessel for the quartering of an observer, or for carrying out observer functions, are so inadequate or unsafe that the health or safety of the observer or the safe operation of the vessel would be jeopardized;

(9) assess and specify the effect which the conservation and management measures of the plan will have on the stocks of naturally spawning anadromous fish in the region;

(10) include, consistent with the other provisions of this Act, conservation and management measures that provide harvest incentives for participants within each gear group to employ fishing practices that result in lower levels of bycatch or in lower levels of the mortality of bycatch;

(11) reserve a portion of the allowable biological catch of the fishery for use in scientific research;

109-479

(12) include management measures in the plan to conserve target and non-target species and habitats, considering the variety of ecological factors affecting fishery populations; and

(14)[sic][15] prescribe such other measures, requirements, or conditions and restrictions as are determined to be necessary and appropriate for the conservation and management of the fishery.

97-453, **104-297**

(c) PROPOSED REGULATIONS.—Proposed regulations which the Council deems necessary or appropriate for the purposes of—

(1) implementing a fishery management plan or plan amendment shall be submitted to the Secretary simultaneously with the plan or amendment under section 304; and

(2) making modifications to regulations implementing a fishery management plan or plan amendment may be submitted to the Secretary at any time after the plan or amendment is approved under section 304.

[15] So in original.

P.L. 109-479, sec. 104(b), MSA § 303 note **16 U.S.C. 1853 note**

EFFECTIVE DATES; APPLICATION TO CERTAIN SPECIES.—The amendment made by subsection (a)(10)[16]—

(1) shall, unless otherwise provided for under an international agreement in which the United States participates, take effect—

(A) in fishing year 2010 for fisheries determined by the Secretary to be subject to overfishing; and

(B) in fishing year 2011 for all other fisheries; and

(2) shall not apply to a fishery for species that have a life cycle of approximately 1 year unless the Secretary has determined the fishery is subject to overfishing of that species; and

(3) shall not limit or otherwise affect the requirements of section 301(a)(1) or 304(e) of the Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 1851(a)(1) or 1854(e), respectively).

109-479

SEC. 303A. LIMITED ACCESS PRIVILEGE PROGRAMS. **16 U.S.C. 1853a**

(a) IN GENERAL.—After the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, a Council may submit, and the Secretary may approve, for a fishery that is managed under a limited access system, a limited access privilege program to harvest fish if the program meets the requirements of this section.

(b) NO CREATION OF RIGHT, TITLE, OR INTEREST.—Limited access privilege, quota share, or other limited access system authorization established, implemented, or managed under this Act—

(1) shall be considered a permit for the purposes of sections 307, 308, and 309;

(2) may be revoked, limited, or modified at any time in accordance with this Act, including revocation if the system is found to have jeopardized the sustainability of the stock or the safety of fishermen;

(3) shall not confer any right of compensation to the holder of such limited access privilege, quota share, or other such limited access system authorization if it is revoked, limited, or modified;

(4) shall not create, or be construed to create, any right, title, or interest in or to any fish before the fish is harvested by the holder; and

(5) shall be considered a grant of permission to the holder of the limited access privilege or quota share to engage in activities permitted by such limited access privilege or quota share.

[16] Section 104(a)(10) of P.L. 109-479 added section 303(a)(15).

(c) REQUIREMENTS FOR LIMITED ACCESS PRIVILEGES.—

(1) IN GENERAL.—Any limited access privilege program to harvest fish submitted by a Council or approved by the Secretary under this section shall—

(A) if established in a fishery that is overfished or subject to a rebuilding plan, assist in its rebuilding;

(B) if established in a fishery that is determined by the Secretary or the Council to have over-capacity, contribute to reducing capacity;

(C) promote—
(i) fishing safety;
(ii) fishery conservation and management; and
(iii) social and economic benefits;

(D) prohibit any person other than a United States citizen, a corporation, partnership, or other entity established under the laws of the United States or any State, or a permanent resident alien, that meets the eligibility and participation requirements established in the program from acquiring a privilege to harvest fish, including any person that acquires a limited access privilege solely for the purpose of perfecting or realizing on a security interest in such privilege;

(E) require that all fish harvested under a limited access privilege program be processed on vessels of the United States or on United States soil (including any territory of the United States);

(F) specify the goals of the program;

(G) include provisions for the regular monitoring and review by the Council and the Secretary of the operations of the program, including determining progress in meeting the goals of the program and this Act, and any necessary modification of the program to meet those goals, with a formal and detailed review 5 years after the implementation of the program and thereafter to coincide with scheduled Council review of the relevant fishery management plan (but no less frequently than once every 7 years);

(H) include an effective system for enforcement, monitoring, and management of the program, including the use of observers or electronic monitoring systems;

(I) include an appeals process for administrative review of the Secretary's decisions regarding initial allocation of limited access privileges;

(J) provide for the establishment by the Secretary, in consultation with appropriate Federal agencies, for an information collection and review process to provide any additional information needed to determine whether any illegal acts of anti-competition, anti-trust, price collusion, or price fixing have occurred among regional fishery associations or persons receiving limited access privileges under the program; and

(K) provide for the revocation by the Secretary of limited access privileges held by any person found to have violated the antitrust laws of the United States.

(2) WAIVER.—The Secretary may waive the requirement of paragraph (1)(E) if the Secretary determines that—

(A) the fishery has historically processed the fish outside of the United States; and

(B) the United States has a seafood safety equivalency agreement with the country where processing will occur.

(3) FISHING COMMUNITIES.—

(A) IN GENERAL.—

(i) ELIGIBILITY.—To be eligible to participate in a limited access privilege program to harvest fish, a fishing community shall—

(I) be located within the management area of the relevant Council;

(II) meet criteria developed by the relevant Council, approved by the Secretary, and published in the Federal Register;

(III) consist of residents who conduct commercial or recreational fishing, processing, or fishery-dependent support businesses within the Council's management area; and

(IV) develop and submit a community sustainability plan to the Council and the Secretary that demonstrates how the plan will address the social and economic development needs of coastal communities, including those that have not historically had the resources to participate in the fishery, for approval based on criteria developed by the Council that have been approved by the Secretary and published in the Federal Register.

(ii) FAILURE TO COMPLY WITH PLAN.—The Secretary shall deny or revoke limited access privileges granted under this section for any person who fails to comply with the requirements of the community sustainability plan. Any limited access privileges denied or revoked under this section may be reallocated to other eligible members of the fishing community.

(B) PARTICIPATION CRITERIA.—In developing participation criteria for eligible communities under this paragraph, a Council shall consider—

(i) traditional fishing or processing practices in, and dependence on, the fishery;

(ii) the cultural and social framework relevant to the fishery;

(iii) economic barriers to access to fishery;

(iv) the existence and severity of projected economic and social impacts associated with implementation of limited access privilege programs on harvesters, captains, crew, processors, and other businesses substantially dependent upon the fishery in the region or subregion;

(v) the expected effectiveness, operational transparency, and equitability of the community sustainability plan; and

(vi) the potential for improving economic conditions in remote coastal communities lacking resources to participate in harvesting or processing activities in the fishery.

(4) REGIONAL FISHERY ASSOCIATIONS.—

(A) IN GENERAL.—To be eligible to participate in a limited access privilege program to harvest fish, a regional fishery association shall—

(i) be located within the management area of the relevant Council;

(ii) meet criteria developed by the relevant Council, approved by the Secretary, and published in the Federal Register;

(iii) be a voluntary association with established by-laws and operating procedures;

(iv) consist of participants in the fishery who hold quota share that are designated for use in the specific region or subregion covered by the regional fishery association, including commercial or recreational fishing, processing, fishery-dependent support businesses, or fishing communities;

(v) not be eligible to receive an initial allocation of a limited access privilege but may acquire such privileges after the initial allocation, and may hold the annual fishing privileges of any limited access privileges it holds or the annual fishing privileges that is [sic][17] members contribute; and

(vi) develop and submit a regional fishery association plan to the Council and the Secretary for approval based on criteria developed by the Council that have been approved by the Secretary and published in the Federal Register.

(B) FAILURE TO COMPLY WITH PLAN.—The Secretary shall deny or revoke limited access privileges granted under this section to any person participating in a regional fishery association who fails to comply with the requirements of the regional fishery association plan.

[17] So in original.

(C) PARTICIPATION CRITERIA.—In developing participation criteria for eligible regional fishery associations under this paragraph, a Council shall consider—

(i) traditional fishing or processing practices in, and dependence on, the fishery;

(ii) the cultural and social framework relevant to the fishery;

(iii) economic barriers to access to fishery;

(iv) the existence and severity of projected economic and social impacts associated with implementation of limited access privilege programs on harvesters, captains, crew, processors, and other businesses substantially dependent upon the fishery in the region or subregion;

(v) the administrative and fiduciary soundness of the association; and

(vi) the expected effectiveness, operational transparency, and equitability of the fishery association plan.

(5) ALLOCATION.—In developing a limited access privilege program to harvest fish a Council or the Secretary shall—

(A) establish procedures to ensure fair and equitable initial allocations, including consideration of—

(i) current and historical harvests;

(ii) employment in the harvesting and processing sectors;

(iii) investments in, and dependence upon, the fishery; and

(iv) the current and historical participation of fishing communities;

(B) consider the basic cultural and social framework of the fishery, especially through—

(i) the development of policies to promote the sustained participation of small owner-operated fishing vessels and fishing communities that depend on the fisheries, including regional or port-specific landing or delivery requirements; and

(ii) procedures to address concerns over excessive geographic or other consolidation in the harvesting or processing sectors of the fishery;

(C) include measures to assist, when necessary and appropriate, entry-level and small vessel owner-operators, captains, crew, and fishing communities through set-asides of harvesting allocations, including providing privileges, which may include set-asides or allocations of harvesting privileges, or economic assistance in the purchase of limited access privileges;

(D) ensure that limited access privilege holders do not acquire an excessive share of the total limited access privileges in the program by—

(i) establishing a maximum share, expressed as a percentage of the total limited access privileges, that a limited access privilege holder is permitted to hold, acquire, or use; and

(ii) establishing any other limitations or measures necessary to prevent an inequitable concentration of limited access privileges; and

(E) authorize limited access privileges to harvest fish to be held, acquired, used by, or issued under the system to persons who substantially participate in the fishery, including in a specific sector of such fishery, as specified by the Council.

(6) PROGRAM INITIATION.—

(A) LIMITATION.—Except as provided in subparagraph (D), a Council may initiate a fishery management plan or amendment to establish a limited access privilege program to harvest fish on its own initiative or if the Secretary has certified an appropriate petition.

(B) PETITION.—A group of fishermen constituting more than 50 percent of the permit holders, or holding more than 50 percent of the allocation, in the fishery for which a limited access privilege program to harvest fish is sought, may submit a petition to the Secretary requesting that the relevant Council or Councils with authority over the fishery be authorized to initiate the development of the program. Any such petition shall clearly state the fishery to which the limited access privilege program would apply. For multispecies permits in the Gulf of Mexico, only those participants who have substantially fished the species proposed to be included in the limited access program shall be eligible to sign a petition for such a program and shall serve as the basis for determining the percentage described in the first sentence of this subparagraph.

(C) CERTIFICATION BY SECRETARY.—Upon the receipt of any such petition, the Secretary shall review all of the signatures on the petition and, if the Secretary determines that the signatures on the petition represent more than 50 percent of the permit holders, or holders of more than 50 percent of the allocation in the fishery, as described by subparagraph (B), the Secretary shall certify the petition to the appropriate Council or Councils.

(D) NEW ENGLAND AND GULF REFERENDUM.—

(i) Except as provided in clause (iii) for the Gulf of Mexico commercial red snapper fishery, the New England and Gulf Councils may not submit, and the Secretary may not approve or implement, a fishery management plan or amendment that creates an individual fishing quota program, including a Secretarial plan, unless such a system, as ultimately developed, has been approved by more than 2⁄3 of those voting in a referendum among eligible permit holders, or other persons described in clause (v), with respect to the New England Council, and by a majority of those voting in the referendum among eligible permit holders with respect to the Gulf Council. For multispecies permits in the Gulf of Mexico, only those participants who have substantially fished the species proposed to be included in the individual fishing quota program shall be eligible to vote in such a referendum. If an individual fishing quota program fails to be approved by the requisite number of those voting, it may be revised and submitted for approval in a subsequent referendum.

(ii) The Secretary shall conduct a referendum under this subparagraph, including notifying all persons eligible to participate in the referendum and making available to them information concerning the schedule, procedures, and eligibility requirements for the referendum process and the proposed individual fishing quota program. Within 1 year after the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, the Secretary shall publish guidelines and procedures to determine procedures and voting eligibility requirements for referenda and to conduct such referenda in a fair and equitable manner.

(iii) The provisions of section 407(c) of this Act shall apply in lieu of this subparagraph for an individual fishing quota program for the Gulf of Mexico commercial red snapper fishery.

(iv) Chapter 35 of title 44, United States Code, (commonly known as the Paperwork Reduction Act) does not apply to the referenda conducted under this subparagraph.

(v) The Secretary shall promulgate criteria for determining whether additional fishery participants are eligible to vote in the New England referendum described in clause (i) in order to ensure that crew members who derive a significant percentage of their total income from the fishery under the proposed program are eligible to vote in the referendum.

(vi) In this subparagraph, the term ‘individual fishing quota’ does not include a sector allocation.

(7) TRANSFERABILITY.—In establishing a limited access privilege program, a Council shall—

(A) establish a policy and criteria for the transferability of limited access privileges (through sale or lease), that is consistent with the policies adopted by the Council for the fishery under paragraph (5); and

(B) establish, in coordination with the Secretary, a process for monitoring of transfers (including sales and leases) of limited access privileges.

(8) PREPARATION AND IMPLEMENTATION OF SECRETARIAL PLANS.—This subsection also applies to a plan prepared and implemented by the Secretary under section 304(c) or 304(g).

(9) ANTITRUST SAVINGS CLAUSE.—Nothing in this Act shall be construed to modify, impair, or supersede the operation of any of the antitrust laws. For purposes of the preceding sentence, the term ‘antitrust laws’ has the meaning given such term in subsection (a) of the first section of the Clayton Act, except that such term includes section 5 of the Federal Trade Commission Act to the extent that such section 5 applies to unfair methods of competition.

(d) AUCTION AND OTHER PROGRAMS.—In establishing a limited access privilege program, a Council shall consider, and may provide, if appropriate, an auction system or other program to collect royalties for the initial, or any subsequent, distribution of allocations in a limited access privilege program if—

(1) the system or program is administered in such a way that the resulting distribution of limited access privilege shares meets the program requirements of this section; and

(2) revenues generated through such a royalty program are deposited in the Limited Access System Administration Fund established by section 305(h)(5)(B) and available subject to annual appropriations.

(e) COST RECOVERY.—In establishing a limited access privilege program, a Council shall—

(1) develop a methodology and the means to identify and assess the management, data collection and analysis, and enforcement programs that are directly related to and in support of the program; and

(2) provide, under section 304(d)(2), for a program of fees paid by limited access privilege holders that will cover the costs of management, data collection and analysis, and enforcement activities.

(f) CHARACTERISTICS.—A limited access privilege established after the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006 is a permit issued for a period of not more than 10 years that—

(1) will be renewed before the end of that period, unless it has been revoked, limited, or modified as provided in this subsection;

(2) will be revoked, limited, or modified if the holder is found by the Secretary, after notice and an opportunity for a hearing under section 554 of title 5, United States Code, to have failed to comply with any term of the plan identified in the plan as cause for revocation, limitation, or modification of a permit, which may include conservation requirements established under the plan;

(3) may be revoked, limited, or modified if the holder is found by the Secretary, after notice and an opportunity for a hearing under section 554 of title 5, United States Code, to have committed an act prohibited by section 307 of this Act; and

(4) may be acquired, or reacquired, by participants in the program under a mechanism established by the Council if it has been revoked, limited, or modified under paragraph (2) or (3).

(g) LIMITED ACCESS PRIVILEGE ASSISTED PURCHASE PROGRAM.—

(1) IN GENERAL.—A Council may submit, and the Secretary may approve and implement, a program which reserves up to 25 percent of any fees collected from a fishery under section 304(d)(2) to be used, pursuant to section 53706(a)(7) of title 46, United States Code, to issue obligations that aid in financing—

(A) the purchase of limited access privileges in that fishery by fishermen who fish from small vessels; and

(B) the first-time purchase of limited access privileges in that fishery by entry level fishermen.

(2) ELIGIBILITY CRITERIA.—A Council making a submission under paragraph (1) shall recommend criteria, consistent with the provisions of this Act, that a fisherman must meet to qualify for guarantees under subparagraphs (A) and (B) of paragraph (1) and the portion of funds to be allocated for guarantees under each subparagraph.

(h) EFFECT ON CERTAIN EXISTING SHARES AND PROGRAMS.—Nothing in this Act, or the amendments made by the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, shall be construed to require a reallocation or a reevaluation of individual quota shares, processor quota shares, cooperative programs, or other quota programs, including sector allocation in effect before the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006.

(i) TRANSITION RULES.—

(1) IN GENERAL.—The requirements of this section shall not apply to any quota program, including any individual quota program, cooperative program, or sector allocation for which a Council has taken final action or which has been submitted by a Council to the Secretary, or approved by the Secretary, within 6 months after the date of enactment of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006, except that—

(A) the requirements of section 303(d) of this Act in effect on the day before the date of enactment of that Act shall apply to any such program;

(B) the program shall be subject to review under subsection (c)(1)(G) of this section not later than 5 years after the program implementation; and

(C) nothing in this subsection precludes a Council from incorporating criteria contained in this section into any such plans.

(2) PACIFIC GROUNDFISH PROPOSALS.—The requirements of this section, other than subparagraphs (A) and (B) of subsection (c)(1) and subparagraphs (A), (B), and (C) of paragraph (1) of this subsection, shall not apply to any proposal authorized under section 302(f) of the Magnuson-Stevens Fishery Conservation and Management Reauthorization Act of 2006 that is submitted within the timeframe prescribed by that section.

P.L. 109-479, sec. 106(e), MSA § 303A note **16 U.S.C. 1853a note**

APPLICATION WITH AMERICAN FISHERIES ACT.—Nothing in section 303A of the Magnuson-Stevens Fishery Conservation and Management Act (16 U.S.C. 1801 et seq.), as added by subsection (a) [P.L. 109-479], shall be construed to modify or supersede any provision of the American Fisheries Act (46 U.S.C. 12102 note; 16 U.S.C. 1851 note; et alia).

P.L. 104-297, sec. 108(i), MSA § 303 note

EXISTING QUOTA PLANS.—Nothing in this Act [P.L.104-297] or the amendments made by this Act shall be construed to require a reallocation of individual fishing quotas under any individual fishing quota program approved by the Secretary before January 4, 1995.

SEC. 304. ACTION BY THE SECRETARY 16 U.S.C. 1854

104-297

(a) REVIEW OF PLANS.—

(1) Upon transmittal by the Council to the Secretary of a fishery management plan or plan amendment, the Secretary shall—

(A) immediately commence a review of the plan or amendment to determine whether it is consistent with the national standards, the other provisions of this Act, and any other applicable law; and

(B) immediately publish in the Federal Register a notice stating that the plan or amendment is available and that written information, views, or comments of interested persons on the plan or amendment may be submitted to the Secretary during the 60-day period beginning on the date the notice is published.

(2) In undertaking the review required under paragraph (1), the Secretary shall—

(A) take into account the information, views, and comments received from interested persons;

(B) consult with the Secretary of State with respect to foreign fishing; and

(C) consult with the Secretary of the department in which the Coast Guard is operating with respect to enforcement at sea and to fishery access adjustments referred to in section 303(a)(6).

(3) The Secretary shall approve, disapprove, or partially approve a plan or amendment within 30 days of the end of the comment period under paragraph (1) by written notice to the Council. A notice of disapproval or partial approval shall specify—

(A) the applicable law with which the plan or amendment is inconsistent;

(B) the nature of such inconsistencies; and

(C) recommendations concerning the actions that could be taken by the Council to conform such plan or amendment to the requirements of applicable law.

If the Secretary does not notify a Council within 30 days of the end of the comment period of the approval, disapproval, or partial approval of a plan or amendment, then such plan or amendment shall take effect as if approved.

Title 50: Wildlife and Fisheries

PART 622—FISHERIES OF THE CARIBBEAN, GULF, AND SOUTH ATLANTIC
Subpart C—Management Measures

§ 622.41 Species specific limitations.

(a) *Aquacultured live rock.* In the Gulf or South Atlantic EEZ:

(1) Aquacultured live rock may be harvested only under a permit, as required under §622.4(a)(3)(iii), and aquacultured live rock on a site may be harvested only by the person, or his or her employee, contractor, or agent, who has been issued the aquacultured live rock permit for the site. A person harvesting aquacultured live rock is exempt from the prohibition on taking prohibited coral for such prohibited coral as attaches to aquacultured live rock.

(2) The following restrictions apply to individual aquaculture activities:

(i) No aquaculture site may exceed 1 acre (0.4 ha) in size.

(ii) Material deposited on the aquaculture site—

(A) May not be placed over naturally occurring reef outcrops, limestone ledges, coral reefs, or vegetated areas.

(B) Must be free of contaminants.

(C) Must be nontoxic.

(D) Must be placed on the site by hand or lowered completely to the bottom under restraint that is, not allowed to fall freely.

(E) Must be placed from a vessel that is anchored.

(F) In the Gulf EEZ, must be distinguishable, geologically or otherwise (for example, be indelibly marked or tagged), from the naturally occurring substrate.

(G) In the South Atlantic EEZ, must be geologically distinguishable from the naturally occurring substrate and, in addition, may be indelibly marked or tagged.

(iii) A minimum setback of at least 50 ft (15.2 m) must be maintained from natural vegetated or hard bottom habitats.

(3) Mechanically dredging or drilling, or otherwise disturbing, aquacultured live rock is prohibited, and aquacultured live rock may be harvested only by hand. In addition, the following activities are prohibited in the South Atlantic: Chipping of aquacultured live rock in the EEZ, possession of chipped aquacultured live rock in or from the EEZ, removal of allowable octocoral or prohibited coral from aquacultured live rock in or from the EEZ, and possession of prohibited coral not attached to aquacultured live rock or allowable octocoral, while aquacultured live rock is in possession. See the definition of “Allowable octocoral” for clarification of the distinction between allowable octocoral and live rock. For the purposes of this paragraph (a)(3), chipping means breaking up reefs, ledges, or rocks into fragments, usually by means of a chisel and hammer.

(4) Not less than 24 hours prior to harvest of aquacultured live rock, the owner or operator of the harvesting vessel must provide the following information to the NMFS Office for Law Enforcement, Southeast Region, St. Petersburg, FL, by telephone (727–824–5344):

(b) *Caribbean reef fish anchoring restriction.* The owner or operator of any fishing vessel, recreational or commercial, that fishes for or possesses Caribbean reef fish in or from the Caribbean EEZ must ensure that the vessel uses only an anchor retrieval system that recovers the anchor by its crown, thereby preventing the anchor from dragging along the bottom during recovery. For a grapnel hook, this could include an incorporated anchor rode reversal bar that runs parallel along the shank, which allows the rode to reverse and slip back toward the crown. For a fluke- or plow-type anchor, a trip line consisting of a line from the crown of the anchor to a surface buoy would be required.

(c) *Coastal migratory pelagic fish —(1) Authorized gear.* Subject to the prohibitions on gear/methods specified in §622.31, the following are the only fishing gears that may be used in the Gulf, Mid-Atlantic, and South Atlantic EEZ in directed fisheries for coastal migratory pelagic fish:

(i) King mackerel, Atlantic migratory group—

(A) North of 34°37.3' N. lat., the latitude of Cape Lookout Light, NC—all gear except drift gillnet and long gillnet.

(B) South of 34°37.3' N. lat.—automatic reel, bandit gear, handline, and rod and reel.

(ii) King mackerel, Gulf migratory group—hook-and-line gear and, in the southern Florida west coast subzone only, run-around gillnet. (See §622.42(c)(1)(i)(A)(*3*) for a description of the southern Florida west coast subzone.)

(iii) Spanish mackerel, Atlantic migratory group—automatic reel, bandit gear, handline, rod and reel, cast net, run-around gillnet, and stab net.

(iv) Spanish mackerel, Gulf migratory group—all gear except drift gillnet, long gillnet, and purse seine.

(v) Cobia in the Mid-Atlantic and South Atlantic EEZ and little tunny in the South Atlantic EEZ south of 34°37.3' N. lat.—automatic reel, bandit gear, handline, rod and reel, and pelagic longline.

(vi) Cero in the South Atlantic EEZ and little tunny in the South Atlantic EEZ north of 34°37.3' N. lat.—all gear except drift gillnet and long gillnet.

(vii) Bluefish, cero, cobia, dolphin, and little tunny in the Gulf EEZ—all gear except drift gillnet and long gillnet.

(2) *Unauthorized gear.* Gear types other than those specified in paragraph (c)(1) of this section are unauthorized gear and the following possession limitations apply:

(i) *Long gillnets.* A vessel with a long gillnet on board in, or that has fished on a trip in, the Gulf, Mid-Atlantic, or South Atlantic EEZ may not have on board on that trip a coastal migratory pelagic fish.

(ii) *Drift gillnets.* A vessel with a drift gillnet on board in, or that has fished on a trip in, the Gulf EEZ may not have on board on that trip a coastal migratory pelagic fish.

(iii) *Other unauthorized gear.* Except as specified in paragraph (c)(2)(iv) of this section, a person aboard a vessel with unauthorized gear other than a drift gillnet in the Gulf EEZ or a long gillnet on board in, or that has fished in, the EEZ where such gear is not authorized in paragraph (c)(1) of this section, is subject to the bag limit for king and Spanish mackerel specified in §622.39(c)(1)(ii) and to the limit on cobia specified in §622.32(c)(1).

(iv) *Exception for king mackerel in the Gulf EEZ.* The provisions of this paragraph (c)(2)(iv) apply to king mackerel taken in the Gulf EEZ and to such king mackerel possessed in the Gulf. Paragraph (c)(2)(iii) of this section notwithstanding, a person aboard a vessel that has a valid commercial permit for king mackerel is not subject to the bag limit for king mackerel when the vessel has on board on a trip unauthorized gear other than a drift gillnet in the Gulf EEZ, a long gillnet, or a run-around gillnet in an area other than the southern Florida west coast subzone. Thus, the following applies to a vessel that has a commercial permit for king mackerel:

(A) Such vessel may not use unauthorized gear in a directed fishery for king mackerel in the Gulf EEZ.

(B) If such a vessel has a drift gillnet or a long gillnet on board or a run-around gillnet in an area other than the southern Florida west coast subzone, no king mackerel may be possessed.

(C) If such a vessel has unauthorized gear on board other than a drift gillnet in the Gulf EEZ, a long gillnet, or a run-around gillnet in an area other than the southern Florida west coast subzone, the possession of king mackerel taken incidentally is restricted only by the closure provisions of §622.43(a) (3) and the trip limits specified in §622.44(a). See also paragraph (c)(4) of this section regarding the purse seine incidental catch allowance of king mackerel.

(3) *Gillnets —(i) King mackerel.* The minimum allowable mesh size for a gillnet used to fish in the Gulf, Mid-Atlantic, or South Atlantic EEZ for king mackerel is 4.75 inches (12.1 cm), stretched mesh. A vessel in such EEZ, or having fished on a trip in such EEZ, with a gillnet on board that has a mesh size less than 4.75 (12.1 cm) inches, stretched mesh, may not possess on that trip an incidental catch of king mackerel that exceeds 10 percent, by number, of the total lawfully possessed Spanish mackerel on board.

(ii) *Spanish mackerel.* (A) The minimum allowable mesh size for a gillnet used to fish for Spanish mackerel in the Gulf, Mid-Atlantic, or South Atlantic EEZ is 3.5 inches (8.9 cm), stretched mesh.

(*1*) A vessel in the Gulf EEZ, or having fished on a trip in the Gulf EEZ, with a gillnet on board that has a mesh size less than 3.5 inches (8.9 cm), stretched mesh, may not possess on that trip any Spanish mackerel.

(*2*) A vessel in the South Atlantic or Mid-Atlantic EEZ, or having fished on a trip in such EEZ, with a gillnet on board that has a mesh size less than 3.5 inches (8.9 cm), stretched mesh, may possess or land on the day of that trip no more than 500 lb (227 kg) of incidentally caught Spanish mackerel.

(B) On board a vessel with a valid Spanish mackerel permit that is fishing for Spanish mackerel in, or that possesses Spanish mackerel in or from, the South Atlantic EEZ off Florida north of 25°20.4' N. lat., which is a line directly east from the Miami-Dade/Monroe County, FL, boundary—

(*1*) No person may fish with, set, place in the water, or have on board a gillnet with a float line longer than 800 yd (732 m).

(*2*) No person may fish with, set, or place in the water more than one gillnet at any one time.

(*3*) No more than two gillnets, including any net in use, may be possessed at any one time; provided, however, that if two gillnets, including any net in use, are possessed at any one time, they must have stretched mesh sizes (as allowed under the regulations) that differ by at least .25 inch (.64 cm).

(*4*) No person may soak a gillnet for more than 1 hour. The soak period begins when the first mesh is placed in the water and ends either when the first mesh is retrieved back on board the vessel or the gathering of the gillnet is begun to facilitate retrieval on board the vessel, whichever occurs first; providing that, once the first mesh is retrieved or the gathering is begun, the retrieval is continuous until the gillnet is completely removed from the water.

(*5*) The float line of each gillnet possessed, including any net in use, must have the distinctive floats specified in §622.6(b)(2).

(4) *Purse seine incidental catch allowance.* A vessel in the EEZ, or having fished in the EEZ, with a purse seine on board will not be considered as fishing, or having fished, for king or Spanish mackerel in violation of a prohibition of purse seines under paragraph (c)(2) of this section, in violation of the possession limits under paragraph (c)(2)(iii) of this section, or, in the case of king mackerel from the Atlantic migratory group, in violation of a closure effected in accordance with §622.43(a), provided the king mackerel on board does not exceed 1 percent, or the Spanish mackerel on board does not exceed 10 percent, of all fish on board the vessel. Incidental catch will be calculated by number and/or weight of fish. Neither calculation may exceed the allowable percentage. Incidentally caught king or Spanish mackerel are counted toward the quotas provided for under §622.42(c) and are subject to the prohibition of sale under §622.43(a)(3)(iii).

(d) *South Atlantic snapper-grouper —(1) Authorized gear.* Subject to the gear restrictions specified in §622.31, the following are the only gear types authorized in a directed fishery for snapper-grouper in the South Atlantic EEZ: Bandit gear, bottom longline, buoy gear, handline, rod and reel, sea bass pot, and spearfishing gear.

(2) *Unauthorized gear.* All gear types other than those specified in paragraph (d)(1) of this section are unauthorized gear and the following possession and transfer limitations apply.

(i) A vessel with trawl gear on board that fishes in the EEZ on a trip may possess no more than 200 lb (90.7 kg) of South Atlantic snapper-grouper, excluding wreckfish, in or from the EEZ on that trip. It is a rebuttable presumption that a vessel with more than 200 lb (90.7 kg) of South Atlantic snapper-grouper, excluding wreckfish, on board harvested such fish in the EEZ.

(ii) Except as specified in paragraphs (d)(3) through (d)(5) of this section, a person aboard a vessel with unauthorized gear on board, other than trawl gear, that fishes in the EEZ on a trip is limited on that trip to:

(A) South Atlantic snapper-grouper species for which a bag limit is specified in §622.39(d)(1)—the bag limit.

(B) All other South Atlantic snapper-grouper—zero.

(iii) South Atlantic snapper-grouper on board a vessel with unauthorized gear on board may not be transferred at sea, regardless of where such transfer takes place, and such snapper-grouper may not be transferred in the EEZ.

(iv) No vessel may receive at sea any South Atlantic snapper-grouper from a vessel with unauthorized gear on board, as specified in paragraph (d)(2)(iii) of this section.

(3) *Possession alowance regarding sink nets off North Carolina.* A vessel that has on board a commercial permit for South Atlantic snapper-grouper, excluding wreckfish, that fishes in the EEZ off North Carolina with a sink net on board, may retain, without regard to the limits specified in paragraph (d)(2)(ii) of this section, otherwise legal South Atlantic snapper-grouper taken with bandit gear, buoy gear, handline, rod and reel, or sea bass pot. For the purpose of this paragraph (d)(3), a sink net is a gillnet with stretched mesh measurements of 3 to 4.75 inches (7.6 to 12.1 cm) that is attached to the vessel when deployed.

(4) *Possession allowance regarding bait nets.* A vessel that has on board a commercial permit for South Atlantic snapper-grouper, excluding wreckfish, that fishes in the South Atlantic EEZ with no more than one bait net on board, may retain, without regard to the limits specified in paragraph (d)(2)(ii) of this section, otherwise legal South Atlantic snapper-grouper taken with bandit gear, buoy gear, handline, rod and reel, or sea bass pot. For the purpose of this paragraph (d)(4), a bait net is a gillnet not exceeding 50 ft (15.2 m) in length or 10 ft (3.1 m) in height with stretched

mesh measurements of 1.5 inches (3.8 cm) or smaller that is attached to the vessel when deployed.

(5) *Possession allowance regarding cast nets.* A vessel that has on board a commercial permit for South Atlantic snapper-grouper, excluding wreckfish, that fishes in the South Atlantic EEZ with a cast net on board, may retain, without regard to the limits specified in paragraph (d)(2)(ii) of this section, otherwise legal South Atlantic snapper-grouper taken with bandit gear, buoy gear, handline, rod and reel, or sea bass pot. For the purpose of this paragraph (d)(5), a cast net is a cone-shaped net thrown by hand and designed to spread out and capture fish as the weighted circumference sinks to the bottom and comes together when pulled by a line.

(6) *Longline species limitation.* A vessel that has on board a valid Federal commercial permit for South Atlantic snapper-grouper, excluding wreckfish, that fishes in the EEZ on a trip with a longline on board, may possess only the following South Atlantic snapper-grouper: snowy grouper, warsaw grouper, yellowedge grouper, misty grouper, golden tilefish, blueline tilefish, and sand tilefish. For the purpose of this paragraph, a vessel is considered to have a longline on board when a power-operated longline hauler, a cable of diameter suitable for use in the longline fishery on any reel, and gangions are on board. Removal of any one of these three elements constitutes removal of a longline.

(e) *South Atlantic golden crab.* Traps are the only fishing gear authorized in directed fishing for golden crab in the South Atlantic EEZ. Golden crab in or from the South Atlantic EEZ may not be retained on board a vessel possessing or using unauthorized gear.

(f) *Caribbean queen conch.* In the Caribbean EEZ, no person may harvest queen conch by diving while using a device that provides a continuous air supply from the surface.

(g) *BRD requirement for Gulf and South Atlantic shrimp .* On a shrimp trawler in the Gulf EEZ or South Atlantic EEZ, each net that is rigged for fishing must have a BRD installed that is listed in paragraph (g) (2) of this section and is certified or provisionally certified for the area in which the shrimp trawler is located, unless exempted as specified in paragraphs (g)(1)(i) through (iv) of this section. A trawl net is rigged for fishing if it is in the water, or if it is shackled, tied, or otherwise connected to a sled, door, or other device that spreads the net, or to a tow rope, cable, pole, or extension, either on board or attached to a shrimp trawler.

(1) *Exemptions from BRD requirement —(i) Royal red shrimp exemption .* A shrimp trawler is exempt from the requirement to have a certified or provisionally certified BRD installed in each net provided that at least 90 percent (by weight) of all shrimp on board or offloaded from such trawler are royal red shrimp.

(ii) *Try net exemption .* A shrimp trawler is exempt from the requirement to have a certified or provisionally certified BRD installed in a single try net with a headrope length of 16 ft (4.9 m) or less provided the single try net is either placed immediately in front of another net or is not connected to another net.

(iii) *Roller trawl exemption .* A shrimp trawler is exempt from the requirement to have a certified or provisionally certified BRD installed in up to two rigid-frame roller trawls that are 16 ft (4.9 m) or less in length used or possessed on board. A rigid-frame roller trawl is a trawl that has a mouth formed by a rigid frame and a grid of rigid vertical bars; has rollers on the lower horizontal part of the frame to allow the trawl to roll over the bottom and any obstruction while being towed; and has no doors, boards, or similar devices attached to keep the mouth of the trawl open.

(iv) *BRD certification testing exemption .* A shrimp trawler that is authorized by the RA to participate in the pre-certification testing phase or to test a BRD in the EEZ for possible certification, has such written authorization on board, and is conducting such test in accordance with the “Bycatch Reduction Device Testing Manual” is granted a limited exemption from the BRD requirement specified in this paragraph (g). The exemption from the BRD requirement is limited to those trawls that are being used in the certification trials. All other trawls rigged for fishing must be equipped with certified or provisionally certified BRDs.

(2) *Procedures for certification and decertification of BRDs .* The process for the certification of BRDs consists of two phases--an optional pre-certification phase and a required certification phase. The RA may also provisionally certify a BRD.

(i) *Pre-certification .* The pre-certification phase allows a person to test and evaluate a new BRD design for up to 60 days without being subject to the observer requirements and rigorous testing requirements specified for certification testing in the “Bycatch Reduction Device Testing Manual.”

(A) A person who wants to conduct pre-certification phase testing must submit an application to the RA, as specified in the “Bycatch Reduction Device Testing Manual.” The “Bycatch Reduction Device Testing Manual”, which is available from the RA, upon request, contains the application forms.

(B) After reviewing the application, the RA will determine whether to issue a letter of authorization (LOA) to conduct pre-certification trials upon the vessel specified in the application. If the RA authorizes precertification, the RA's LOA must be on board the vessel during any trip involving the BRD testing.

(ii) *Certification .* A person who proposes a BRD for certification for use in the Gulf EEZ or South Atlantic EEZ must submit an application to test such BRD, conduct the testing, and submit the results of the test in accordance with the "Bycatch Reduction Device Testing Manual." The RA will issue a LOA to conduct certification trials upon the vessel specified in the application if the RA finds that: The operation plan

submitted with the application meets the requirements of the "Bycatch Reduction Device Testing Manual'; the observer identified in the application is qualified; and the results of any pre-certification trials conducted have been reviewed and deemed to indicate a reasonable scientific basis for

conducting certification testing. If authorization to conduct certification trials is denied, the RA will provide a letter of explanation to the applicant, together with relevant recommendations to address the deficiencies resulting in the denial. To be certified for use in the fishery, the BRD candidate must successfully demonstrate a 30 percent reduction in total weight of finfish bycatch. In addition, the BRD candidate must satisfy the following conditions: There is at least a 50–percent probability the true reduction rate of the BRD candidate meets the bycatch reduction criterion and there is no more than a 10–percent probability the true reduction rate of the BRD candidate is more than 5 percentage points less than the bycatch reduction criterion. If a BRD meets both conditions, consistent with the "Bycatch Reduction Device Testing Manual", NMFS, through appropriate rulemaking procedures, will add the BRD to the list of certified BRDs in paragraph (g)(3) of this section; and provide the specifications for the newly certified BRD, including any special conditions deemed appropriate based on the certification testing results.

(iii) *Provisional certification.* Based on data provided consistent with the "Bycatch Reduction Device Testing Manual", the RA may provisionally certify a BRD if there is at least a 50–percent probability the true reduction rate of the BRD is no more than 5 percentage points less than the bycatch reduction criterion, i.e. 25 percent reduction in total weight of finfish bycatch. Through appropriate rulemaking procedures, NMFS will add the BRD to the list of provisionally certified BRDs in paragraph (g)(3) of this section; and provide the specifications for the BRD, including any special conditions deemed appropriate based on the certification testing results. A provisional certification is effective for 2 years from the date of publication of the notification in the Federal Register announcing the provisional certification.

(iv) *Decertification .* The RA will decertify a BRD if NMFS determines the BRD does not meet the requirements for certification or provisional certification. Before determining whether to decertify a BRD, the RA will notify the appropriate Fishery Management Council in writing, and the public will be provided an opportunity to comment on the advisability of any proposed decertification. The RA will consider any comments from the Council and public, and if the RA elects to decertify the BRD, the RA will proceed with decertification via appropriate rulemaking.

(3) *Certified and provisionally certified BRDs —(i) Certified BRDS .* The following BRDs are certified for use in the Gulf EEZ and South Atlantic EEZ unless indicated otherwise. Specifications of these certified BRDs are contained in Appendix D to this part.

(A) Fisheye.

(B) Gulf fisheye.

(C) Jones-Davis.

(D) Modified Jones-Davis.

(E) Expanded mesh.

(F) Extended funnel -South Atlantic EEZ only.

(ii) *Provisionally certified BRDs .* The following BRDs are provisionally certified for use in the areas and for the time periods indicated. Specifications of these provisionally certified BRDs are contained in Appendix D to this part.

(A) Extended funnel- Gulf EEZ only; through February 16, 2010.

(B) Composite panel -Gulf EEZ and South Atlantic EEZ; through February 16, 2010.

(h) [Reserved]

(i) Pre-certification. The pre-certification phase allows a person to test and evaluate a new BRD design for up to 60 days without being subject to the observer requirements and rigorous testing requirements specified for certification testing in the *Gulf Of Mexico Bycatch Reduction Device Testing Protocol Manual .*

(A) A person who wants to conduct pre-certification phase testing must submit an application, as specified in the *Gulf Of Mexico Bycatch Reduction Device Testing Protocol Manual,* to the RA. The *Gulf Of Mexico Bycatch Reduction Device Testing Protocol Manual,* which is available from the RA, upon request, contains the application forms.

(B) After reviewing the application, the RA will determine whether to issue a letter of authorization (LOA) to conduct pre-certification trials upon the vessel specified in the application. The RA will issue a precertification phase LOA if the BRD design is substantially unlike any BRD design previously determined not to meet the BRD certification criterion or, if the design is substantially similar to a BRD design previously determined not to meet the BRD certification criteria, and the application demonstrates that the design could meet the certification criterion through design revision or upon retesting (e.g., the application shows that statistical results could be improved upon retesting by such things as using a larger sample size than that previously used). If the RA authorizes pre-certification, the RA's letter of authorization must be on board the vessel during any trip involving the BRD testing.

(ii) *Certification.* A person who proposes a BRD for certification for use in the Gulf EEZ must submit an application to test such BRD, conduct the testing, and submit the results of the test in accordance with the *Gulf Of Mexico Bycatch Reduction Device Testing Protocol Manual.* The RA will issue a LOA to conduct certification trials upon the vessel specified in the application if the RA finds that: The test plan meets the requirements of the protocol; the observer identified in the application is qualified and has no current or prior financial relationship with the entity seeking BRD certification; the application presents a BRD candidate substantially unlike BRDs previously determined not to meet the current bycatch reduction criterion, or the applicant has shown good cause for reconsideration (such as the likelihood of improved statistical results yielded from a larger sample size than that previously used); and for BRDs not previously tested for certification, the results of any pre-certification trials conducted have been reviewed and deemed to indicate a reasonable scientific basis for conducting certification testing. If authorization to conduct certification trials is denied, the RA will provide a letter of explanation to the applicant, together with relevant recommendations to address the deficiencies resulting in the denial. If a BRD meets the certification criterion, as determined under the testing protocol, NMFS will publish a notice in the Federal Register adding the BRD to the list of certified BRDs in paragraph (h)(2) of this section providing the specifications for the newly certified BRD, including any special conditions deemed appropriate based on the certification testing results.

(iii) A shrimp trawler that is authorized to participate in the pre-certification phase or to test a BRD in the EEZ for possible certification has such written authorization on board and is conducting such test in accordance with the *Gulf Of Mexico Bycatch Reduction Device Testing Protocol Manual* is granted a limited exemption from the BRD requirement specified in paragraph (h)(1) of this section. The exemption from the BRD requirement is limited to those trawls that are being used in the certification trials. All other trawls rigged for fishing must be equipped with certified BRDs.

(i) Gulf reef fish exhibiting trap rash. Possession of Gulf reef fish in or from the Gulf EEZ that exhibit trap rash is prima facie evidence of illegal trap use and is prohibited. For the purpose of this paragraph, trap rash is defined as physical damage to fish that characteristically results from contact with wire fish traps. Such damage includes, but is not limited to, broken fin spines, fin rays, or teeth; visually obvious loss of scales; and cuts or abrasions on the body of the fish, particularly on the head, snout, or mouth.

(j) *Rock shrimp in the South Atlantic off Georgia and Florida.* The minimum mesh size for the cod end of a rock shrimp trawl net in the South Atlantic EEZ off Georgia and Florida is 1 7/8 inches (4.8 cm), stretched mesh. This minimum mesh size is required in at least the last 40 meshes forward of the cod end drawstring (tie-off rings), and smaller-mesh bag liners are not allowed. A vessel that has a trawl net on board that does not meet these requirements may not possess a rock shrimp in or from the South Atlantic EEZ off Georgia and Florida.

(k)*Pelagic sargassum.* The minimum allowable mesh size for a net used to fish for pelagic sargassum in the South Atlantic EEZ is 4.0 inches (10.2 cm), stretched mesh, and such net must be attached to a frame no larger than 4 ft by 6 ft (1.2 m by 1.8 m). A vessel in the South Atlantic EEZ with a net on board that does not meet these requirements may not possess any pelagic sargassum.

(l) *Atlantic dolphin and wahoo —(1) Authorized gear.* The following are the only authorized gear types in the fisheries for dolphin and wahoo in the Atlantic EEZ: Automatic reel, bandit gear, handline, pelagic longline, rod and reel, and spearfishing gear (including powerheads). A person aboard a vessel in the Atlantic EEZ that has on board gear types other than authorized gear types may not possess a dolphin or wahoo.

(2) [Reserved]

(m) *Required gear in the Gulf reef fish fishery .* For a person on board a vessel to fish for Gulf reef fish in the Gulf EEZ, the vessel must possess on board and such person must use the gear as specified in paragraphs (m)(1) through (m)(3) of this section.

(1) *Non-stainless steel circle hooks .* Non-stainless steel circle hooks are required when fishing with natural baits.

(2) *Dehooking device .* At least one dehooking device is required and must be used to remove hooks embedded in Gulf reef fish with minimum damage. The hook removal device must be constructed to allow the hook to be secured and the barb shielded without re-engaging during the removal process. The dehooking end must be blunt, and all edges rounded. The device must be of a size appropriate to secure the range of hook sizes and styles used in the Gulf reef fish fishery.

(3) *Venting tool .* At least one venting tool is required and must be used to deflate the swim bladders of Gulf reef fish

to release the fish with minimum damage. This tool must be a sharpened, hollow instrument, such as a hypodermic syringe with the plunger removed, or a 16–gauge needle fixed to a hollow wooden dowel. A tool such as a knife or an ice-pick may not be used. The venting tool must be inserted into the fish at a 45–degree angle approximately 1 to 2 inches (2.54 to 5.08 cm) from the base of the pectoral fin. The tool must be inserted just deep enough to release the gases, so that the fish may be released with minimum damage.

[61 FR 34934, July 3, 1996, as amended at 61 FR 43959, Aug. 27, 1996; 61 FR 65484, Dec. 13, 1996; 62 FR 18539, Apr. 16, 1997; 63 FR 10568, Mar. 4, 1998; 63 FR 18144, Apr. 14, 1998; 63 FR 38303, July 16, 1998; 64 FR 3628, Jan. 25, 1999; 64 FR 36781, July 8, 1999; 64 FR 37694, July 13, 1999; 64 FR 43941, Aug. 12, 1999; 64 FR 45459, Aug. 20, 1999; 64 FR 52428, Sept. 29, 1999; 64 FR 59126, Nov. 2, 1999; 64 FR 68935, Dec. 9, 1999; 65 FR 16340, Mar. 28, 2000; 65 FR 52957, Aug. 31, 2000; 65 FR 61116, Oct. 16, 2000; 68 FR 2196, Jan. 16, 2003; 68 FR 57378, Oct. 3, 2003; 69 FR 1541, Jan. 9, 2004; 69 FR 30242, May 27, 2004; 70 FR 62082, Oct. 28, 2005; 70 FR 73388, Dec. 12, 2005; 73 FR 411, Jan. 3, 2008; 73 FR 8223, Feb. 13, 2008; 73 FR 5128, Jan. 29, 2008]

COMPUTER SECURITY ACT OF 1987
Public Law 100-235 (H.R. 145)
January 8, 1988

SECTION 1. SHORT TITLE

The Act may be cited as the "Computer Security Act of 1987".

SEC. 2 PURPOSE

(a) IN GENERAL.-The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) SPECIFIC PURPOSES.-The purposes of this Act are--

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901, (15 U.S.C. 271-278h), is amended--

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof: "; and", and by inserting after such paragraph the following:

"(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections: "SEC. 20. (a) The National Bureau of Standards shall--

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code.

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except--

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

The primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that

contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized--

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)--

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of--

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a) (1) and (a) (3) , and

"(2) performing research and conducting studies under subsection (b)(5), the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section--

"(1) the term computer system'--

"A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes--

" (i) computers;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

"(2) the term 'Federal computer system'--

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any

information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

"**SEC. 21.** (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at lease one of whom is representative of small or medium sized companies in such industries;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be--

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate Committees of the Congress.

"(c) The term of office of each member of the Board shall be four years, except that-

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

"(g) As used in this section, the terms 'computer system' and 'Federal computer

system' have the meanings given in section 20(d) of this Act."; and

"(3) by adding at the end thereof the following new section:

"**SEC. 23.** This Act may be cited as the National Bureau of Standards Act."

SEC. 4 AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

"(2) The head of a Federal agency may employ standards for the cost effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that ar more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effect implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act.".

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

(a) In General.--Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be--

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES.--Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed--

(1) to enhance employees' awareness of the threats to and vulnerability of

computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.--Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION-
Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.--Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude or the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

SEC. 7. DEFINITIONS.

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

SEC. 8. RULES OF CONSTRUCTION OF ACT.

Nothing in this Act, or in any amendment made by this Act, shall be construed--

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is--

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

Subtitle G—Government Information Security Reform

SEC. 1061. COORDINATION OF FEDERAL INFORMATION POLICY.

Chapter 35 of title 44, United States Code, is amended by inserting at the end the following new subchapter:

"SUBCHAPTER II—INFORMATION SECURITY

"§ 3531. Purposes

"The purposes of this subchapter are the following:

"(1) To provide a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets.

"(2)(A) To recognize the highly networked nature of the Federal computing environment including the need for Federal Government interoperability and, in the implementation of improved security management measures, assure that opportunities for interoperability are not adversely affected.

"(B) To provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities.

"(3) To provide for development and maintenance of minimum controls required to protect Federal information and information systems.

"(4) To provide a mechanism for improved oversight of Federal agency information security programs.

"§ 3532. Definitions

"(a) Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

"(b) In this subchapter:

"(1) The term 'information technology' has the meaning given that term in section 5002 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1401).

"(2) The term 'mission critical system' means any telecommunications or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, that—

"(A) is defined as a national security system under section 5142 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1452);

"(B) is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy; or

"(C) processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

"§ 3533. Authority and functions of the Director

"(a)(1) The Director shall establish governmentwide policies for the management of programs that—

"(A) support the cost-effective security of Federal information systems by promoting security as an integral component of each agency's business operations; and

"(B) include information technology architectures as defined under section 5125 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1425).

"(2) Policies under this subsection shall—

"(A) be founded on a continuing risk management cycle that recognizes the need to—

"(i) identify, assess, and understand risk; and

"(ii) determine security needs commensurate with the level of risk;

"(B) implement controls that adequately address the risk;

"(C) promote continuing awareness of information security risk; and

"(D) continually monitor and evaluate policy and control effectiveness of information security practices.

"(b) The authority under subsection (a) includes the authority to—

"(1) oversee and develop policies, principles, standards, and guidelines for the handling of Federal information and information resources to improve the efficiency and effectiveness of governmental operations, including principles, policies, and guidelines for the implementation of agency responsibilities under applicable law for ensuring the privacy, confidentiality, and security of Federal information;

"(2) consistent with the standards and guidelines promulgated under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100–235; 101 Stat. 1729), require Federal agencies to identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency;

"(3) direct the heads of agencies to—

"(A) identify, use, and share best security practices;

"(B) develop an agencywide information security plan;

"(C) incorporate information security principles and practices throughout the life cycles of the agency's information systems; and

"(D) ensure that the agency's information security plan is practiced throughout all life cycles of the agency's information systems;

"(4) oversee the development and implementation of standards and guidelines relating to security controls for Federal computer systems by the Secretary of Commerce through the National Institute of Standards and Technology under section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441) and section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3);

"(5) oversee and coordinate compliance with this section in a manner consistent with—

"(A) sections 552 and 552a of title 5;

"(B) sections 20 and 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3 and 278g–4);

"(C) section 5131 of the Clinger-Cohen Act of 1996 (40 U.S.C. 1441);

"(D) sections 5 and 6 of the Computer Security Act of 1987 (40 U.S.C. 1441 note; Public Law 100–235; 101 Stat. 1729); and

"(E) related information management laws; and

"(6) take any authorized action under section 5113(b)(5) of the Clinger-Cohen Act of 1996 (40 U.S.C. 1413(b)(5)) that the Director considers appropriate, including any action involving the budgetary process or appropriations management process, to enforce accountability of the head of an agency for information resources management, including the requirements of this subchapter, and for the investments made by the agency in information technology, including—

"(A) recommending a reduction or an increase in any amount for information resources that the head of the agency proposes for the budget submitted to Congress under section 1105(a) of title 31;

"(B) reducing or otherwise adjusting apportionments and reapportionments of appropriations for information resources; and

"(C) using other authorized administrative controls over appropriations to restrict the availability of funds for information resources.

"(c) The authorities of the Director under this section (other than the authority described in subsection (b)(6))—

"(1) shall be delegated to the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2);

"(2) shall be delegated to the Secretary of Defense in the case of systems described under subparagraph (C) of section 3532(b)(2) that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense; and

"(3) in the case of all other Federal information systems, may be delegated only to the Deputy Director for Management of the Office of Management and Budget.

"§ 3534. Federal agency responsibilities

"(a) The head of each agency shall—

"(1) be responsible for—

"(A) adequately ensuring the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets;

"(B) developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency; and

"(C) ensuring that the agency's information security plan is practiced throughout the life cycle of each agency system;

"(2) ensure that appropriate senior agency officials are responsible for—

"(A) assessing the information security risks associated with the operations and assets for programs and systems over which such officials have control;

"(B) determining the levels of information security appropriate to protect such operations and assets; and

"(C) periodically testing and evaluating information security controls and techniques;

"(3) delegate to the agency Chief Information Officer established under section 3506, or a comparable official in an agency not covered by such section, the authority to administer all functions under this subchapter including—

"(A) designating a senior agency information security official who shall report to the Chief Information Officer or a comparable official;

"(B) developing and maintaining an agencywide information security program as required under subsection (b);

"(C) ensuring that the agency effectively implements and maintains information security policies, procedures, and control techniques;

"(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

"(E) assisting senior agency officials concerning responsibilities under paragraph (2);

"(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

"(5) ensure that the agency Chief Information Officer, in coordination with senior agency officials, periodically—

"(A)(i) evaluates the effectiveness of the agency information security program, including testing control techniques; and

"(ii) implements appropriate remedial actions based on that evaluation; and

"(B) reports to the agency head on—

"(i) the results of such tests and evaluations; and

"(ii) the progress of remedial actions.

"(b)(1) Each agency shall develop and implement an agencywide information security program to provide information security for the operations and assets of the agency, including operations and assets provided or managed by another agency.

"(2) Each program under this subsection shall include—

"(A) periodic risk assessments that consider internal and external threats to—

"(i) the integrity, confidentiality, and availability of systems; and

"(ii) data supporting critical operations and assets;

"(B) policies and procedures that—

"(i) are based on the risk assessments required under subparagraph (A) that cost-effectively reduce information security risks to an acceptable level; and

"(ii) ensure compliance with—

"(I) the requirements of this subchapter;

"(II) policies and procedures as may be prescribed by the Director; and

"(III) any other applicable requirements;

"(C) security awareness training to inform personnel of—

"(i) information security risks associated with the activities of personnel; and

"(ii) responsibilities of personnel in complying with agency policies and procedures designed to reduce such risks;

"(D) periodic management testing and evaluation of the effectiveness of information security policies and procedures;

"(E) a process for ensuring remedial action to address any significant deficiencies; and

"(F) procedures for detecting, reporting, and responding to security incidents, including—

"(i) mitigating risks associated with such incidents before substantial damage occurs;

"(ii) notifying and consulting with law enforcement officials and other offices and authorities;

"(iii) notifying and consulting with an office designated by the Administrator of General Services within the General Services Administration; and

"(iv) notifying and consulting with an office designated by the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President for incidents involving systems described under subparagraphs (A) and (B) of section 3532(b)(2).

"(3) Each program under this subsection is subject to the approval of the Director and is required to be reviewed at least annually by agency program officials in consultation with the Chief Information Officer. In the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), the Director shall delegate approval authority under this paragraph to the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President.

"(c)(1) Each agency shall examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to—

"(A) annual agency budgets;

"(B) information resources management under subchapter I of this chapter;

"(C) performance and results based management under the Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.);

"(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 through 2805 of title 39; and

"(E) financial management under—

"(i) chapter 9 of title 31, United States Code, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101–576) (and the amendments made by that Act);

"(ii) the Federal Financial Management Improvement Act of 1996 (31 U.S.C. 3512 note) (and the amendments made by that Act); and

"(iii) the internal controls conducted under section 3512 of title 31.

"(2) Any significant deficiency in a policy, procedure, or practice identified under paragraph (1) shall be reported as a material

weakness in reporting required under the applicable provision of law under paragraph (1).

"(d)(1) In addition to the requirements of subsection (c), each agency, in consultation with the Chief Information Officer, shall include as part of the performance plan required under section 1115 of title 31 a description of—

"(A) the time periods; and

"(B) the resources, including budget, staffing, and training, which are necessary to implement the program required under subsection (b)(1).

"(2) The description under paragraph (1) shall be based on the risk assessment required under subsection (b)(2)(A).

"§ 3535. Annual independent evaluation

"(a)(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency.

"(2) Each evaluation by an agency under this section shall include—

"(A) testing of the effectiveness of information security control techniques for an appropriate subset of the agency's information systems; and

"(B) an assessment (made on the basis of the results of the testing) of the compliance with—

"(i) the requirements of this subchapter; and

"(ii) related information security policies, procedures, standards, and guidelines.

"(3) The Inspector General or the independent evaluator performing an evaluation under this section may use an audit, evaluation, or report relating to programs or practices of the applicable agency.

"(b)(1)(A) Subject to subparagraph (B), for agencies with Inspectors General appointed under the Inspector General Act of 1978 (5 U.S.C. App.) or any other law, the annual evaluation required under this section or, in the case of systems described under subparagraphs (A) and (B) of section 3532(b)(2), an audit of the annual evaluation required under this section, shall be performed by the Inspector General or by an independent evaluator, as determined by the Inspector General of the agency.

"(B) For systems described under subparagraphs (A) and (B) of section 3532(b)(2), the evaluation required under this section shall be performed only by an entity designated by the Secretary of Defense, the Director of Central Intelligence, or another agency head as designated by the President.

"(2) For any agency to which paragraph (1) does not apply, the head of the agency shall contract with an independent evaluator to perform the evaluation.

"(c) Each year, not later than the anniversary of the date of the enactment of this subchapter, the applicable agency head shall submit to the Director—

"(1) the results of each evaluation required under this section, other than an evaluation of a system described under subparagraph (A) or (B) of section 3532(b)(2); and

"(2) the results of each audit of an evaluation required under this section of a system described under subparagraph (A) or (B) of section 3532(b)(2).

"(d)(1) The Director shall submit to Congress each year a report summarizing the materials received from agencies pursuant to subsection (c) in that year.

"(2) Evaluations and audits of evaluations of systems under the authority and control of the Director of Central Intelligence and evaluations and audits of evaluation of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available only to the appropriate oversight committees of Congress, in accordance with applicable laws.

"(e) Agencies and evaluators shall take appropriate actions to ensure the protection of information, the disclosure of which may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws.

"§ 3536. Expiration

"This subchapter shall not be in effect after the date that is two years after the date on which this subchapter takes effect.".

SEC. 1062. RESPONSIBILITIES OF CERTAIN AGENCIES.

(a) DEPARTMENT OF COMMERCE.—Notwithstanding section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) and except as provided under subsection (b), the Secretary of Commerce, through the National Institute of Standards and Technology and with technical assistance from the National Security Agency, as required or when requested, shall—

(1) develop, issue, review, and update standards and guidance for the security of Federal information systems, including development of methods and techniques for security systems and validation programs;

(2) develop, issue, review, and update guidelines for training in computer security awareness and accepted computer security practices, with assistance from the Office of Personnel Management;

(3) provide agencies with guidance for security planning to assist in the development of applications and system security plans for such agencies;

(4) provide guidance and assistance to agencies concerning cost-effective controls when interconnecting with other systems; and

(5) evaluate information technologies to assess security vulnerabilities and alert Federal agencies of such vulnerabilities as soon as those vulnerabilities are known.

(b) DEPARTMENT OF DEFENSE AND THE INTELLIGENCE COMMUNITY.—

(1) IN GENERAL.—Notwithstanding any other provision of this subtitle (including any amendment made by this subtitle)—

(A) the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President, shall, consistent with their respective authorities—

(i) develop and issue information security policies, standards, and guidelines for systems described under subparagraphs (A) and (B) of section 3532(b)(2) of title 44, United States Code (as added by section 1061 of this Act), that provide more stringent protection, to

the maximum extent practicable, than the policies, principles, standards, and guidelines required under section 3533 of such title (as added by such section 1061); and

(ii) ensure the implementation of the information security policies, principles, standards, and guidelines described under clause (i); and

(B) the Secretary of Defense shall, consistent with his authority—

(i) develop and issue information security policies, standards, and guidelines for systems described under subparagraph (C) of section 3532(b)(2) of title 44, United States Code (as added by section 1061 of this Act), that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that provide more stringent protection, to the maximum extent practicable, than the policies, principles, standards, and guidelines required under section 3533 of such title (as added by such section 1061); and

(ii) ensure the implementation of the information security policies, principles, standards, and guidelines described under clause (i).

(2) MEASURES ADDRESSED.—The policies, principles, standards, and guidelines developed by the Secretary of Defense and the Director of Central Intelligence under paragraph (1) shall address the full range of information assurance measures needed to protect and defend Federal information and information systems by ensuring their integrity, confidentiality, authenticity, availability, and nonrepudiation.

(c) DEPARTMENT OF JUSTICE.—The Attorney General shall review and update guidance to agencies on—

(1) legal remedies regarding security incidents and ways to report to and work with law enforcement agencies concerning such incidents; and

(2) lawful uses of security techniques and technologies.

(d) GENERAL SERVICES ADMINISTRATION.—The Administrator of General Services shall—

(1) review and update General Services Administration guidance to agencies on addressing security considerations when acquiring information technology; and

(2) assist agencies in—

(A) fulfilling agency responsibilities under section 3534(b)(2)(F) of title 44, United States Code (as added by section 1061 of this Act); and

(B) the acquisition of cost-effective security products, services, and incident response capabilities.

(e) OFFICE OF PERSONNEL MANAGEMENT.—The Director of the Office of Personnel Management shall—

(1) review and update Office of Personnel Management regulations concerning computer security training for Federal civilian employees;

(2) assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and computer security best practices; and

(3) work with the National Science Foundation and other agencies on personnel and training initiatives (including scholarships and fellowships, as authorized by law) as necessary to ensure that the Federal Government—

(A) has adequate sources of continuing information security education and training available for employees; and

(B) has an adequate supply of qualified information security professionals to meet agency needs.

(f) INFORMATION SECURITY POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES.—

(1) ADOPTION OF POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES OF OTHER AGENCIES.—The policies, principles, standards, and guidelines developed under subsection (b) by the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President may be adopted, to the extent that such policies are consistent with policies and guidance developed by the Director of the Office of Management and Budget and the Secretary of Commerce—

(A) by the Director of the Office of Management and Budget, as appropriate, for application to the mission critical systems of all agencies; or

(B) by an agency head, as appropriate, for application to the mission critical systems of that agency.

(2) DEVELOPMENT OF MORE STRINGENT POLICIES, PRINCIPLES, STANDARDS, AND GUIDELINES.—To the extent that such policies are consistent with policies and guidance developed by the Director of the Office of Management and Budget and the Secretary of Commerce, an agency may develop and implement information security policies, principles, standards, and guidelines that provide more stringent protection than those required under section 3533 of title 44, United States Code (as added by section 1061 of this Act), or subsection (a) of this section.

(g) ATOMIC ENERGY ACT OF 1954.—Nothing in this subtitle (including any amendment made by this subtitle) shall supersede any requirement made by, or under, the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.). Restricted Data or Formerly Restricted Data shall be handled, protected, classified, downgraded, and declassified in conformity with the Atomic Energy Act of 1954 (42 U.S.C. 2011 et seq.).

SEC. 1063. RELATIONSHIP OF DEFENSE INFORMATION ASSURANCE PROGRAM TO GOVERNMENT-WIDE INFORMATION SECURITY PROGRAM.

(a) CONSISTENCY OF REQUIREMENTS.—Subsection (b) of section 2224 of title 10, United States Code, is amended—

(1) by striking "(b) OBJECTIVES OF THE PROGRAM.—" and inserting "(b) OBJECTIVES AND MINIMUM REQUIREMENTS.—(1)"; and

(2) by adding at the end the following:

"(2) The program shall at a minimum meet the requirements of sections 3534 and 3535 of title 44.".

(b) ADDITION TO ANNUAL REPORT.—Subsection (e) of such section is amended by adding at the end the following new paragraph:

"(7) A summary of the actions taken in the administration of sections 3534 and 3535 of title 44 within the Department of Defense.".

SEC. 1064. TECHNICAL AND CONFORMING AMENDMENTS.

(a) TABLE OF SECTIONS.—Chapter 35 of title 44, United States Code, is amended—

(1) in the table of sections—

(A) by inserting after the chapter heading the following:

"SUBCHAPTER I—FEDERAL INFORMATION POLICY";

and

(B) by inserting after the item relating to section 3520 the following:

"SUBCHAPTER II—INFORMATION SECURITY

"Sec.
"3531. Purposes.
"3532. Definitions.
"3533. Authority and functions of the Director.
"3534. Federal agency responsibilities.
"3535. Annual independent evaluation.
"3536. Expiration.";

and

(2) by inserting before section 3501 the following:

"SUBCHAPTER I—FEDERAL INFORMATION POLICY".

(b) REFERENCES TO CHAPTER 35.—Sections 3501 through 3520 of title 44, United States Code, are amended by striking "chapter" each place it appears and inserting "subchapter", except in section 3507(i)(1) of such title.

SEC. 1065. EFFECTIVE DATE.

This subtitle and the amendments made by this subtitle shall take effect 30 days after the date of the enactment of this Act.

Subtitle H—Security Matters

SEC. 1071. LIMITATION ON GRANTING OF SECURITY CLEARANCES.

(a) IN GENERAL.—Chapter 49 of title 10, United States Code, is amended by adding at the end the following new section:

"§ 986. Security clearances: limitations

"(a) PROHIBITION.—After the date of the enactment of this section, the Department of Defense may not grant or renew a security clearance for a person to whom this section applies who is described in subsection (c).

"(b) COVERED PERSONS.—This section applies to the following persons:

"(1) An officer or employee of the Department of Defense.

"(2) A member of the Army, Navy, Air Force, or Marine Corps who is on active duty or is in an active status.

"(3) An officer or employee of a contractor of the Department of Defense.

"(c) PERSONS DISQUALIFIED FROM BEING GRANTED SECURITY CLEARANCES.—A person is described in this subsection if any of the following applies to that person:

Administrative Management and Executive Secretariat

NAO 216-100

PROTECTION OF CONFIDENTIAL FISHERIES STATISTICS Eff: 7/18/94; Iss: 7/26/94

SECTION 1. PURPOSE.

. 01 This Order:

a. prescribes policies and procedures for protecting the confidentiality of data submitted to and collected by the National Oceanic and Atmospheric Administration (NOAA)/National Marine Fisheries Service (NMFS) as authorized or required by law;

b.informs authorized users of their obligations for maintaining the confidentiality of data received by NMFS;

c. provides for operational safeguards to maintain the security of data; and

d. states the penalties provided by law for disclosure of confidential data.

SECTION 2. SCOPE.

This Order covers all confidential data received, collected, maintained, or used by NMFS.

SECTION 3. DEFINITIONS.

. 01 **Access to data** means the freedom or ability to use data, conditioned by a statement of nondisclosure and penalties for unauthorized use.

. 02 **Aggregate or summary form** means data structured so that the identity of the submitter cannot be determined either from the present release of the data or in combination with other releases.

. 03 **Agreement** refers to all binding forms of mutual commitment under a stated set of conditions to achieve a specific objective.

. 04 **Assistant Administrator** means the Assistant Administrator for Fisheries, NOAA, or a designee authorized to have access to confidential data.

. 05 **Authorized Use/User.**

a. **Authorized use** is that specific use authorized under the governing statute, regulation, order, contract or agreement.

b. An **authorized user** is any person who, having the need to collect or use confidential data in the performance of an official activity, has read this Order and has signed a statement of nondisclosure affirming the user's understanding of NMFS obligations with respect to confidential data and the penalties for unauthorized use and disclosure.

. 06 **Confidential data** means data that are identifiable with any person, accepted by the Secretary, and prohibited by law from being disclosed to the public. The term "as used" does not convey data sensitivity for national security purposes [See Executive Order (E.O.) 12356 dated April 2, 1982].

. 07 **Data** refers to information used as a basis for reasoning, discussion, or calculation that a person may submit, either voluntarily or as required by statute or regulation.

. 08 **GC** means the Office of General Counsel, NOAA.

. 09 **Person** means any individual (whether or not a citizen or national of the United States), any corporation, partnership, association, or other entity (whether or not organized or existing under the laws of any State), and any Federal, State, local, or foreign government or any entity of such governments, including Regional Fishery Management Councils (Councils).

.10 **Public** means any person who is not an authorized user.

.11 **Region** means NMFS Regional field offices, Fisheries Science Centers, and associated laboratories.

.12 **Source document** means the document, paper, or electronic format on which data are originally recorded.

.13 **State employee** means any member of a State agency responsible for developing and monitoring the State's program for fisheries or Marine Mammal Protection Act (MMPA) program.

. 14 **Submitter** means any person or the agent of any person who provides data to NMFS either

voluntarily or as required by statute or regulation.

SECTION 4. POLICY.

For data subject to this Order, it is NMFS policy that:

a. confidential data shall only be disclosed to the public if required by the Freedom of Information Act (FOIA), 5 U.S.C. 552, the Privacy Act, 5 U.S.C. 552a, or by court order. Disclosure of data pursuant to a subpoena issued by an agency of competent jurisdiction is a lawful disclosure. Disclosure pursuant to a subpoena must be approved by GC;

b. individual identifiers shall be retained with data, unless the permanent deletion is consistent with the needs of NMFS and good scientific practice [See Section 6.02c]; and

c. a notice is required on all report forms requesting data and must comply with 5 U.S.C. 552a(e)(3) and Paperwork Reduction Act requirements in NAO 216-8, Information Collections and Requirements Needing Office of Management and Budget Clearance. [See E.O. 12600 of June 23, 1987, for additional information regarding the rights of submitters to designate commercial confidential data at the time of submission.]

SECTION 5. OPERATIONAL RESPONSIBILITIES.

. 01 The Regional Director of each region (or, in the case of headquarters, each Office Director) has the responsibility to maintain the confidentiality of all data collected, maintained, and disclosed by the respective region.

. 02 Each region shall submit to the Assistant Administrator specific procedures governing the collection, maintenance, and disclosure of confidential data. These documents shall be compiled as regional handbooks following the guidelines and standards:

a. handbooks are to be developed in detail to ensure the maintenance of confidential data on a functional basis in each region; and

b. handbooks shall be coordinated through the National Data Management Committee (a NMFS group established by the Assistant Administrator to develop data management policies and procedures) and reviewed annually. The regional handbooks will address, at minimum, the contents of Sections 6-7.

SECTION 6. PROCEDURES.

. 01 **Data Collection.** To collect data, the Secretary may use Federal employees, contractor employees, or, pursuant to an agreement, State employees.

a. **General Requirements.**

1. Personnel authorized to collect Federal data must maintain all documents containing confidential data in secure facilities; and

2. may not disclose confidential data, whether recorded or not, to anyone not authorized to receive and handle such data.

b. **Specific Requirements.**

1. Each Federal or contractor employee collecting or processing confidential data will be required to read, date, and sign a statement of nondisclosure, that affirms the employee's understanding of NMFS obligations with respect to confidential data and the penalties for unauthorized use and disclosure of the data. Upon signature, the employee's name will be placed on record as an "authorized user," and the employee will be issued certification.
2. Data collected by a contractor must be transferred timely to authorized Federal employees; no copies of these data may be retained by the contractor. NMFS may permit contractors to retain aggregated data. A data return clause shall be included in the agreement. All procedures applicable to Federal employees must be followed by contractor employees collecting data with Federal authority.

3. Under agreements with the State, each State data collector collecting confidential data will sign a statement at least as protective as the one signed by Federal employees, which affirms that the signer understands the applicable procedures and regulations and the penalties for unauthorized disclosure.

.02 **Maintenance.**

a. Maintenance is defined as the procedures required to keep confidential data secure from the time the source documents are received by NMFS to their ultimate disposition, regardless of format. [See National Institute of Standards and Technology "Computer Security Publications, List 91" for guidance.]

b. Specific procedures in regional handbooks must deal with the following minimum security requirements, as well as any others that may be necessary because of the specific data, equipment, or physical facilities:

1. the establishment of an office or person responsible for evaluating requests for access to data;

2. the identifications of all persons certified as authorized users. These lists shall be kept current and reviewed on an annual basis;

3. the issuance of employee security rules that emphasize the confidential status of certain data and the consequences of unauthorized removal or disclosure;

4. the description of the security procedures used to prevent unauthorized access to and/or removal of confidential data;

5. the development of a catalog/inventory system of all confidential data received including: the type of source document; the authority under which each item of data was collected; any statutory or regulatory restriction(s) which may apply; and routing from the time of receipt until final disposition; and

6. The development of an appropriate coding system for each set of confidential data so that access to data that identifies, or could be used to identify, the person or business of the submitter is controlled by the use of one or more coding system(s). Lists that contain the codes shall be kept secure.

c. The permanent deletion of individual identifiers from a database shall be addressed on a case-by-case basis. Identifiers may only be deleted after:

1. future uses of data have thoroughly been evaluated, e.g., the need for individual landings records for allocating shares under an individual transferable quota program;

2. consultation with the agency(s) collecting data (if other than NMFS), the relevant Council(s), and NMFS Senior Scientist; and

3. concurrence by the Assistant Administrator has been received prior to deletion.

.03 **Access to Data Subject to This Order.**

a. **General Requirements.** In determining whether to grant a request for access to confidential data, the following information shall be taken into consideration:

1. the specific types of data required;

2. the relevance of the data to the intended uses;

3. whether access will be continuous, infrequent, or one-time;

4. an evaluation of the requester's statement of why aggregate or nonconfidential summaries of data would not satisfy the requested needs; and

5. the legal framework for the disclosure, in accordance with GC and this Order.

b. **Within NMFS.** NMFS employees requesting confidential data must have certification as being authorized users for the particular type of data requested.

b. **Councils.** Upon written request by the Council Executive Director:

1. "authorized user" status for confidential data collected under the Magnuson Fishery Conservation and Management Act (Magnuson Act) may be granted to a Council for use by the Council for conservation and management purposes consistent with the approval of the Assistant Administrator as described in 50 CFR 603.5;

2. "authorized user" status for confidential data, collected under the Magnuson Act and MMPA, will be granted to Council employees who are responsible for Fishery Management Plan development and monitoring; and

3. Councils that request access to confidential data must submit, on an annual basis, a copy of their procedures for ensuring the confidentiality of data to the region, or in the case of intercouncil fisheries, regions. The procedures will be evaluated for their effectiveness and, if necessary, changes may be recommended. As part of this procedure, an updated statement of nondisclosure will be included for each employee and member who requires access to confidential data.

d. **States.**

1. Requests from States for confidential data shall be directed in writing to the NMFS office that maintains the source data.

2. Each request will be processed in accordance with any agreement NMFS may have with the State:

(a) confidential data collected **solely** under Federal authority will be provided to a State by NMFS only if the Assistant Administrator finds that the State has authority to protect the confidentiality of the data comparable to, or more stringent than, NMFS' requirements; and

(b) the State will exercise its authority to limit subsequent access and use of the data to those uses allowed by authorities under which the data was collected.

3. If the State has no agreement with NMFS for the collection and exchange of confidential data, the request shall be treated as a public request and disclosure may be denied subject to FOIA or the Privacy Act.

4. Where a State has entered into a cooperative exchange agreement with another State(s), NMFS will facilitate transfer or exchange of State collected data in its possession if:

(a) NMFS has written authorization for data transfer from the head of the collecting State agency; and

(b) the collecting State has provided NMFS a list of authorized users in the recipient State(s); and

(c) the collecting State agrees to hold the United States Government harmless for any suit that may arise from the misuse of the data.

e. **Contractors.**

1. Pursuant to an agreement with NMFS, a NMFS contractor (including universities, Sea Grant investigators, etc.) may be granted "authorized user" status consistent with this Order if the use furthers the mission of NMFS.

2. The region will notify the contractor of its decision on access in writing within 30 calendar days after receipt of the request.

3. Contingent upon approval, the contractor will be provided with details regarding conditions of data access, any costs involved, formats, timing, and security procedures. If the request is denied, the reason(s) for denial will be given by the NMFS office involved. The denial will not preclude NMFS consideration of future requests from the contractor.

4. If access is granted, language in the agreement specifically dealing with confidentiality of data will be required. The language shall include all of the relevant portions of this Order and shall prohibit the further disclosure of the data. No data may be retained beyond the termination date of the agreement; and any disclosure of data derived from the accessed confidential data must be approved by NMFS.

5. Each agreement shall be reviewed by GC prior to its execution, and shall, to the extent possible, be consistent with the model agreement contained in Appendix D (Not included --WebEd).

f. **Submitters.** The Privacy Act allows for data to be released back to the submitter upon receipt and verification of a written request stating the data required.

04. **Requests for Confidential Data.** NMFS is authorized to collect data under various statutes [See Appendix A (Not include --WebEd)]. Two types of statutes govern the disclosure of confidential data collected by the Federal Government, those that contain specific and non-discretionary language within the Act, and those that provide overall guidance to the Federal Government. Sections of these Acts that deal with exceptions to disclosure may be found in Appendix B (Not included -- WebEd).

a. **Magnuson Act and MMPA.**

1. Data collected under 16 U.S.C. 1853 (a) or (b), and 16 U.S.C. 1383a (c),(d),(e),(f),or (h) will be handled in the following manner:

(a) data will only be disclosed to Federal employees and Council employees who are responsible for management plan development and monitoring; State employees pursuant to an agreement with the Secretary that prevents public disclosure of the identity or business of any person; a Council for conservation and management purposes [not applicable for MMPA data] or when required by court order. [See 50 CFR 229.10 and part 603];

(b) Council advisory groups are not permitted access to such confidential data [See 50 CFR 601.27(b)];

(c) requests from States that do not have an agreement with the Secretary will be processed in accordance with the Privacy Act or FOIA; and

(d) data collected by an observer under 16 U.S.C. 1853 (a) or (b) are not considered to have been "submitted to the Secretary by any person," and therefore are not confidential under Section 6.04.a of this Order. Data collected by an observer may be withheld from disclosure under the Privacy Act, or subsections (b)(3),(4),(5),(6), or (7) of FOIA.

2. Confidential data submitted to the Secretary under other Sections of the Magnuson Act or MMPA may only be disclosed in accordance with the Privacy Act or FOIA. Types of data and the collection authority may include among others:

(a) Processed Product Data -- 16 U.S.C. 1854(e);

(b) Fish Meal and Oil, Monthly -- 16 U.S.C. 1854(e);

(c) Data Collected Under State Authority and Provided to NMFS -- 16 U.S.C. 1854(e); and

(d) Tuna-Dolphin Observer Program -- 16 U.S.C. 1361 et seq.

b. **South Pacific Tuna Act.** Data collected under South Pacific Tuna Act 16 U.S.C. 973j is protected from disclosure to the public in accordance with section 973j(b).

c. **Other Statutes.** Confidential data collected under other NMFS programs as authorized by statutes other than South Pacific Tuna Act (16 U.S.C 973j), MMPA (16 U.S.C. 1361 et seq.), and Magnuson Act (16 U.S.C. 1801 et seq.), may only be disclosed to the public in accordance with the Privacy Act and FOIA. Types of data and the collection authority may include among others:

(1) Monthly Cold Storage Fish Report -- 16 U.S.C. 742(a);

(2) Market News Data -- 16 U.S.C. 742(a); and

(3) Seafood Inspection Data -- 7 U.S.C. 1621 et seq.

d. **Special Procedures.**

1. **Cold Storage Summary Reports.** NMFS publishes monthly cold storage holdings of fishery products. Advance knowledge of the content of
these reports could give those who trade in the products an opportunity to gain competitive advantage. Therefore, in addition to the confidential protection provided to individual reports, the monthly summary report will not be disclosed to the public until 3:00 p.m. Eastern Time of the official release date. Release dates for these data are published 1 year in advance in November, and can be obtained from the NMFS Fisheries Statistics Division.

2. **Surplus commodity purchases by USDA.** NMFS and the Department of Agriculture (USDA) have an interagency agreement relating to the purchase of surplus fishery products. NMFS is responsible for providing confidential data and recommendations to the USDA regarding these purchases. Advance knowledge of these data could cause a competitive advantage or disadvantage to the general public, fishing industry, and the program. Therefore, all NMFS personnel engaged in the surplus commodity purchase program will be required to sign a specific "USDA Responsibility Statement." A copy will be maintained in the Office of Trade Services.

3. **Agreements for Disclosure of Confidential Data.** A letter of agreement may authorize the disclosure of confidential data when both the Government and the submitter agree to disclosure of the data. The need to provide security for the data will vary depending on the type of data collected and the form of the disclosure. Disclosure can be undertaken if all the following conditions are met:

(a) the person has agreed in writing to the disclosure and is aware that disclosure is irrevocable;

(b) the recipient has been informed in writing of the sensitivity of the data; and

(c) the wording of the agreement has been approved by GC.

. 05 Disposal. NAO 205-1, NOAA Records Management Program, shall govern the disposition of records covered under this Order.

SECTION 7. PENALTIES.

. 01 **Civil and Criminal.** Persons who make unauthorized disclosure of confidential data may be subject to civil penalties or criminal prosecution under:

a. Trade Secrets Act (18 U.S.C. 1905);

b. Privacy Act (5 U.S.C. 552a(i)(1));

c. Magnuson Act (16 U.S.C. 1858); and

d. MMPA (16 U.S.C. 1375).

. 02 **Conflict of Interest.** Employees are prohibited by Department of Commerce employee conduct regulations [15 CFR part 0] and by ethics regulations applicable to the Executive Branch [5 CFR 2635.703] from using nonpublic information subject to this Order for personal gain, whether or not there is a disclosure to a third party.

. 03 **Disciplinary Action.** Persons may be subject to disciplinary action, including removal, for failure to comply with this Order. Prohibited activities include, but are not limited to, unlawful disclosure or use of the data, and failure to comply with implementing regulations or statutory prohibitions relating to the collection, maintenance, use and disclosure of data covered by this Order.

SECTION 8. EFFECT ON OTHER ISSUANCES. None.

update their own individual information on the internet at *http://www.beaconregistration.noaa.gov.* User ID and user password are set-up with initial Web registration or with a first visit to the Web site.

CONTESTING RECORD PROCEDURES:

Individual beacon owners have access to their database file and have the ability to update or correct information. Other issues are addressed by the system manager who can be contacted at the above address.

RECORD SOURCE CATEGORIES:

The individual on whom the record is maintained provides information to NOAA by either the website or mail. Existing registrations can be updated according to the above processes, by a phone call from the beacon owner, or by rescue coordination center controllers when updated information is collected while processing a case.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: April 11, 2003.

Brenda Dolan,

Department of Commerce, Freedom of Information/Privacy Act Officer.

[FR Doc. E8–8241 Filed 4–16–08; 8:45 am]

BILLING CODE 3510–HR–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration (NOAA)

[Docket No. 080404520–8522–01]

Privacy Act of 1974; System of Records

AGENCY: Department of Commerce.

ACTION: Notice of a new Privacy Act System of Records: COMMERCE/NOAA–19, Permits and Registrations for United States Federally Regulated Fisheries.

SUMMARY: This notice announces the Department of Commerce's (Department's) proposal for a new system of records under the Privacy Act. NOAA's National Marine Fisheries Service (NMFS) is creating a new system of records for permits and non-permit registrations for use with a variety of fisheries management programs. Information will be collected from individuals under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the High Seas Fishing Compliance Act, the American Fisheries Act, the Tuna Conventions Act of 1950, the Atlantic Coastal Fisheries Cooperative Management Act, the Atlantic Tunas Convention Authorization Act, the Northern Pacific Halibut Act, the Antarctic Marine Living Resources Convention Act, International Fisheries Regulations regarding U.S. Vessels Fishing in Colombian Treaty Waters, and the Marine Mammal Protection Act. This new record system is necessary to identify participants in the fisheries and to evaluate the qualifications of the applicants.

DATES: To be considered, written comments must be submitted on or before May 19, 2008. Unless comments are received, the new system of records will become effective as proposed on the date of publication of a subsequent notice in the **Federal Register**.

ADDRESSES: Comments may be mailed to: Ted Hawes, Team Leader, Northeast Permits Team, NOAA's National Marine Fisheries Service, Northeast Regional Office, One Blackburn Drive, Gloucester, MA 01930.

FOR FURTHER INFORMATION CONTACT: Ted Hawes, Team Leader, Northeast Permits Team, NOAA's National Marine Fisheries Service, Northeast Regional Office, One Blackburn Drive, Gloucester, MA 01930.

SUPPLEMENTARY INFORMATION: NMFS is creating a new system of records for permit and non-permit registrations for use with a variety of fisheries management programs. NMFS requires the use of permits or registrations by participants in U.S. federally regulated fisheries. Information collections would be requested from individuals under the authority of the Magnuson-Stevens Fishery Conservation and Management Act, the High Seas Fishing Compliance Act, the American Fisheries Act, the Atlantic Coastal Fisheries Cooperative Management Act, the Tuna Conventions Act of 1950, the Atlantic Tunas Convention Authorization Act, the Northern Pacific Halibut Act, the Antarctic Marine Living Resources Convention Act, and the Marine Mammal Protection Act. The collection of information is necessary to identify participants in these fisheries and to evaluate the qualifications of the applicants. NMFS would collect information from individuals in order to issue, renew, or transfer fishing permits or to make non-permit registrations. The authority for the mandatory collection of the Tax Identification Number (Employer Identification Number or Social Security Number) is the Debt Collection Improvement Act, 31 U.S.C. 7701.

COMMERCE/NOAA–19

SYSTEM NAME:

Permits and Registrations for United States Federally Regulated Fisheries.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATIONS:

NMFS Northeast Region, One Blackburn Drive, Gloucester, MA 01930 (includes Atlantic Highly Migratory Species (HMS) Tuna Dealer permits).

NMFS Southeast Region, 263 13th Avenue South, St. Petersburg, FL 33701 (includes Atlantic HMS International Trade Permit, shark and swordfish vessel permits, shark and swordfish dealer permits).

NMFS Northwest Region, Sustainable Fisheries Division, 7600 Sand Point Way NE., Bldg. #1, Seattle, WA 98115.

NMFS Southwest Region, 501 West Ocean Boulevard, Suite 4200, Long Beach, CA 90802.

NMFS Southwest Fisheries Science Center, 8604 La Jolla Shores Drive, La Jolla, CA 92037 (Pacific Highly Migratory Species database only).

NMFS Pacific Islands Region, 1601 Kapiolani Boulevard, Suite 1110, Honolulu, HI 96814.

NMFS Alaska Region, 709 West Ninth Street, Juneau, AK 99802–1668.

NMFS Office of Science and Technology, 1315 East West Highway, 12th Floor, Silver Spring, MD 20910 (National Saltwater Angler Registry, High Seas Fishing Compliance Act, and Antarctic Marine Living Resources harvesting permit data).

NMFS Office of Sustainable Fisheries, P.O. Drawer 1207, Pascagoula, MS 39567 (Antarctic Marine Living Resources import permit data).

NMFS Office of Sustainable Fisheries, 1315 East West Highway, Room 13130, Silver Spring, MD 20910 (Atlantic HMS Tuna vessel permits, HMS Angling Permit, HMS Charter/headboat permits database).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Owners or holders of a permit or registration as recognized by NMFS, owner agents, vessel owners and/or operators. Individuals who apply for any permit, permit exception, permit exemption or regulation exemption, registration, dedicated access privilege or fishing quota share either initially, annually, or by transfer. Applicants seeking permission to fish in a manner that would otherwise be prohibited in order to conduct experimental fishing. Owners of processing facilities and/or fish dealers. Permit qualifiers (persons whose incomes are used for permit

qualification). Allocation assignees under a Southeast Region individual fishing quota.

CATEGORIES OF RECORDS IN THE SYSTEM:

THIS INFORMATION IS COLLECTED AND/OR MAINTAINED BY ALL REGIONS AND DIVISIONS:

Current permit number, permit status information, type of application, name of applicant and of other individuals on application (vessel owner(s), owner's agent, operator, dealer, corporation members), and position in company (if applicable), corporation name, date of incorporation and articles of incorporation (if applicable), date of birth, address, telephone numbers (business, cell and/or fax), U.S. Coast Guard Certificate of Documentation number or state vessel registration number and date of expiration, Vessel Monitoring System (VMS) activation certification, vessel name, vessel function, vessel characteristics (length, breadth, external markings, hull or superstructure color), gross and net tonnage, type of construction, fuel capacity and type, horsepower (engine, pump), type of product storage. The Tax Identification Number (TIN) (Employer Identification Number (EIN) or Social Security Number (SSN)) is required for all permits, under the authority of the Debt Collection Improvement Act (DCIA), 31 U.S.C. 7701. The primary purpose for requesting the TIN is for the collection and reporting on any delinquent amounts arising out of such person's relationship with the government pursuant to the DCIA.

It is required in subsection (c)(1) that each person doing business with NMFS is to furnish their taxpayer identifying number. For purposes of administering the various NMFS fisheries permit and registration programs, a person shall be considered to be doing business with a federal agency including but not limited to if the person is an applicant for, or recipient of, a federal license, permit, right-of-way, grant, or benefit payment administered by the agency or insurance administered by the agency pursuant to subsection (c)(2)(B) of the DCIA.

ADDITIONAL INFORMATION IS COLLECTED AND/OR MAINTAINED BY INDIVIDUAL REGIONS AND DIVISIONS:

Northeast Region

For transferable permits: Hair and eye color, height and weight, ID-sized photograph, medical records for resolution of permit dispute, enforcement actions, court and legal documents, and permit sanction notices filed by General Counsel, credit card and/or checking account numbers, cancelled checks, tax returns, internal permit number specific to each limited entry permit, baseline specifications on limited entry permit, country, captain's license, State and Federal Dealer Numbers (if applicable), coast on which dealer does business, processing sector, facilities where fish received, vessel landing receipts and records, dealer purchase receipts, bills of sale, type of vessel registration, NMFS unique vessel ID, year vessel built, hailing port, hailing port state, principal port, principal state, vessel operations type (catching and/or processing: For at-sea processing permit), fish hold capacity, passenger capacity, VMS status, crew size, fishery type, fishery management plan and category, maximum days at sea, quota allocation and shares, regional fishery management organization, species or species code, type of gear, gear code and rank, buoy and trap/pot color, number of tags assigned to vessel, number of traps, dredge size and number.

Southeast Region

Fee payment information, business e-mail address, Web site, gender, hair and eye color, height and weight, ID-sized photograph, Dunn and Bradstreet Corporation Number, NMFS internal identification number, county, country, marriage certificate, divorce decree, death certificate, trust documents, probated will, enforcement actions, court and legal documents, and permit sanction notices filed by General Counsel, name of vessel permit applicant if not owner, and relationship to owner, type of vessel ownership, captain's license, original permit, permit payment information, name of permit transferor and number of permit before transfer, permit and vessel sale price (for permit transfers), date of permit transfer signature, notarized sale and lease agreement with lease start and end dates if applicable, income or license qualifier for certain fisheries, Income Qualification Affidavit for income qualified fisheries, U.S. importer number, State and Federal Dealer Numbers (if applicable), plant name and operator, hull identification number, hailing port and hailing port state, year vessel built, location where vessel built, fish hold capacity, live well capacity, radio call sign, vessel communication types and numbers, crew size, passenger capacity, fishery type, quota shares, vessel landing receipts and records, bills of sale, processing facility where fish are received, gear type, species/gear endorsements, buoy/trap color code, number of traps, trap tag number series, trap dimensions, trap mesh size, designated fishing zone, aquaculture reports, site description, material deposited and harvested, value of material, Highly Migratory Species workshop certificate, informational telephone calls recorded with member of public's knowledge, for customer service evaluation and constituent statement records.

Atlantic Highly Migratory Species

Business e-mail, Web site, Dunn and Bradstreet Corporation Number, percent/rank of ownership interest, lease start/end date, income or license qualifier for certain fisheries, U.S. Importer Number (dealers), State and Federal Dealer Numbers (if applicable), processing facility where fish are received, type of vessel registration, hull identification number, passenger capacity, crew size, hailing port, hailing port state, principal port, principal port state, fish hold capacity, year vessel built, fishery type, species or species code, type of fishing gear, gear code.

Northwest Region

Fee payment information, business e-mail address, NMFS internal identification number, ownership rank if applicable, permit payment information, credit card and/or checking account numbers, canceled checks, tax returns, divorce decree, marriage certificate, city and state where married, death certificate, probated will, trust documents, medical records for emergency transfer of certain permits only, enforcement actions, court and legal documents, and permit sanction notices filed by General Counsel, name of permit transferor and number of permit before transfer, period of permit lease, permit price, location where vessel built, fishery type, quota shares, species and gear endorsements, gear code, amount of landed fish or processed fish product, operation as mother ship with start and end date.

Southwest Region

Business e-mail address, applicant's name and relationship to owner or owner manager if not owner or operator, country, Dunn and Bradstreet Corporation Number, other federal, state and commercial licenses held by operator, name of permit transferor and number of permit before transfer, type of vessel (commercial fishing, charter), vessel photograph, hull identification number, hailing port, hailing port state, principal port, principal port state, year vessel built, where vessel built, maximum vessel speed, fish hold capacity, processing equipment, passenger capacity, crew size, international radio call sign, Vessel Monitoring System (VMS) status, dolphin safety gear on board, previous

vessel flag, previous vessel name and effective dates, species/gear endorsements, fishery type, type of fishing gear, gear code, fishing status (active or inactive), intent to make intentional purse seine sets on marine mammals, date, location, and provider of most recent tuna purse seine marine mammal skipper workshop.

Pacific Islands Region

Photograph identification, citizenship, credit card and/or checking account numbers, cancelled checks, owner of checking account from which permit fees paid, enforcement actions, court and legal documents, and permit sanction notices filed by General Counsel, name of permit transferor and number of permit before transfer, International Maritime Organization number, NMFS vessel identification number, international radio call sign, year vessel built, location where vessel built, fishery type, percent of ownership interest, ownership and catch history as basis for exemption eligibility, days at sea allocations, quota shares, vessel landing receipts and records, dealer purchase receipts, bills of sale.

Alaska Region

Business e-mail address, country, NMFS internal identification number, citizenship, reference names, owner beneficiary, death certificate, marriage certificate, divorce decree, trust documents, probated will, medical information for emergency transfer of certain permits only, enforcement actions, court and legal documents, and permit sanction notices filed by General Counsel, credit card and/or bank account numbers, canceled checks, tax returns, name of Alaska Native tribe, community of residence, fishery community organization, community governing body contact person, nonprofit name, community represented by nonprofit, cooperative representative, percent of ownership interest, permit restrictions, quota type, names of other quota holders if affiliated with any cooperative member receiving quota against cap, names and relationship of permit transferor and transferee, transfer eligibility certificate, sector and region before transfer, relationship of transferor and transferee, reason for transfer, broker's name and fee, lien information (if applicable), quota transfer costs, permit financing source, permit fee, sale/lease agreement, period of lease, agreement to return shares (if applicable), for crab rationalization: affidavit that right of first refusal contracts were signed, number of units and pounds of fish transferred, applicable dealer license numbers, processing plant name and identification, operation type and operator, type of vessel registration, State of Alaska registration number, NMFS vessel identification number, hull identification number, hailing port and hailing port state, numbers of existing permits if applicable to current application, documentation of loss or destruction of a vessel, list of vessels in a vessel cooperative, vessel operations type in terms of catching and/or processing, species/gear endorsements for fisheries requiring vessel monitoring systems, fishery type, species or species code, fishery management plan, days at sea allocations, quota shares, type of fishing gear, gear code, vessel landing receipts and records, bills of sale, delivery receipts, dealer purchase receipts, processing sector and facility where fish are received, statement from processor that there is a market for rockfish received from applicant for entry level harvester permit.

High Seas Fishing Compliance Act

Citizenship, internal identification number, percent/rank of ownership interest, hull identification number, vessel photograph, type of vessel registration, year vessel built, where vessel built, fish hold capacity, hailing port, hailing port state, crew size, international radio call sign, previous vessel flag, previous vessel name, fishery type, fishery management plan, regional fishery management organization, type of fishing gear, gear code.

Antarctic Marine Living Resources

Nationality, type of vessel (commercial fishing, charter), where vessel built, year vessel built, fish hold capacity, International Maritime Organization number (if issued), vessel communication types and serial numbers, details of tamper-proof VMS elements, ice classification, processing equipment, international radio call sign, foreign vessel flag, previous vessel flag, previous vessel name, permit number of supporting foreign vessel, crew size, species code, type of fishing gear, information on the known and anticipated impacts of bottom trawling gear on vulnerable marine ecosystems, and the products to be derived from an anticipated catch of krill.

National Saltwater Angler Registry Program

Name, TIN, address, telephone number, designation as owner or operator of for-hire vessel, vessel name and registration/documentation number and a statement of the region(s) in which the registrant fishes.

AUTHORITIES FOR MAINTENANCE OF THE SYSTEM:

Magnuson-Stevens Fishery Conservation and Management Act, 16 U.S.C. 1801 et seq. (Magnuson-Stevens Act); High Seas Fishing Compliance Act of 1995, 16 U.S.C. 5501 et seq; International Fisheries Regulations: Vessels of the United States Fishing in Colombian Treaty Waters: 50 CFR 300.120; the American Fisheries Act, Title II, Public Law No. 105–277; the Atlantic Coastal Fisheries Cooperative Management Act of 1993, 16 U.S.C. 5101–5108, as amended 1996; the Tuna Conventions Act of 1950, 16 U.S.C. 951–961; the Atlantic Tunas Convention Authorization Act, 16 U.S.C., Chapter 16A; the Northern Pacific Halibut Act of 1982, 16 U.S.C. 773 et seq. (Halibut Act), the Antarctic Marine Living Resources Convention Act of 1984, 16 U.S.C. 2431–2444; the Marine Mammal Protection Act, 16 U.S.C. 1361; and the Debt Collection Improvement Act, 31 U.S.C. 7701.

PURPOSE(S):

This information will allow NMFS to identify owners and holders of permits and non-permit registrations, identify vessel owners and operators, evaluate requests by applicants and current participants, or agency actions, related to the issuance, renewal, transfer, revocation, suspension or modification of a permit or registration.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSE OF SUCH USES:

These records may be disclosed as follows.

1. In the event that a system of records maintained by the Department to carry out its functions indicates a violation or potential violation of law or contract, whether civil, criminal or regulatory in nature and whether arising by general statute or particular program statute or contract, rule, regulation, or order issued pursuant thereto, or the necessity to protect an interest of the Department, the relevant records in the system of records may be referred to the appropriate agency, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute or contract, rule, regulation, or order issued pursuant thereto, or protecting the interest of the Department.

2. A record from this system of records may be disclosed in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing

counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed to a Member of Congress submitting a request involving an individual when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed to the Department of Justice in connection with determining whether the Freedom of Information Act (5 U.S.C. 552) requires disclosure thereof.

5. A record in this system will be disclosed to the Department of Treasury for the purpose of reporting and recouping delinquent debts owed the United States pursuant to the Debt Collection Improvement Act of 1996.

6. A record in this system may be disclosed to the Department of Homeland Security for the purpose of determining the admissibility of certain seafood imports into the United States.

7. A record in this system of records may be disclosed to a contractor of the Department having need for the information in the performance of the contract but not operating a system of records within the meaning of 5 U.S.C. 552a(m).

8. A record in this system of records may be disclosed to approved persons at the state or interstate level within the applicable Marine Fisheries Commission for the purpose of co-managing a fishery or for making determinations about eligibility for permits when state data are all or part of the basis for the permits.

9. A record in this system of records may be disclosed to the applicable Fishery Management Council (Council) staff and contractors tasked with the development of analyses to support Council decisions about Fishery Management Programs.

10. A record in this system of records may be disclosed to the applicable NMFS Observer Program for purpose of identifying current permit owners and vessels and making a random assignment of observers to vessels in a given fishing season.

11. A record in this system of records may be disclosed to the applicable Regional or International Fisheries Management Body for the purpose of identifying current permit owners and vessels pursuant to applicable statutes or regulations and/or conservation and management measures adopted by a Regional or International Fisheries Management Body, such as: the Food and Agriculture Organization of the United Nations, Commission for the Conservation of Antarctic Marine Living Resources, Inter-American Tropical Tuna Commission, International Pacific Halibut Commission, and International Commission for the Conservation of Atlantic Tunas.

12. A record in this system of records may be disclosed to appropriate agencies, entities, and persons when: (1) It is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that, as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosure to consumer reporting agencies pursuant to 5 U.S.C. 552a(b)(12) may be made from this system to ''consumer reporting agencies'' as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) and the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Computerized database; CDs; paper records stored in file folders in locked metal cabinets and/or locked rooms.

RETRIEVABILITY:

Records are organized and retrieved by NMFS internal identification number, name of entity, permit number, vessel name or identification number, or plant name. Records can be accessed by any file element or any combination thereof.

SAFEGUARDS:

The system of records is stored in a building with doors that are locked during and after business hours. Visitors to the facility must register with security guards and must be accompanied by federal personnel at all times. Records are stored in a locked room and/or a locked file cabinet. Electronic records containing Privacy Act information are protected by a user identification/password. The user identification/password is issued to individuals as authorized by authorized personnel.

All electronic information disseminated by NOAA adheres to the standards set out in Appendix III, Security of Automated Information Resources, OMB Circular A–130; the Computer Security Act (15 U.S.C. 278g–3 and 278g–4); and the Government Information Security Reform Act, Public Law 106–398; and follows NIST SP 800–18, Guide for Developing Security Plans for Federal Information Systems; NIST SP 800–26, Security Self-Assessment Guide for Information Technology Systems; and NIST SP 800–53, Recommended Security Controls for Federal Information Systems.

RETENTION AND DISPOSAL:

All records are retained and disposed of in accordance with National Archive and Records Administration regulations (36 CFR Chapter XII, Subchapter B—Records Management); Departmental directives and comprehensive records schedules; NOAA Administrative Order 205–01; and the NMFS Records Disposition Schedule, Chapter 1500.

SYSTEM MANAGER(S) AND ADDRESSES:

Division Chief, Fisheries Statistics Office, NMFS Northeast Region, NMFS Northeast Region, One Blackburn Drive, Gloucester, MA 01930.

Assistant Regional Administrator for Operations, Management, and Information Services, NMFS Southeast Region, 263 13th Avenue South, St. Petersburg, FL 33701.

Permit Team Leader, NMFS Northwest Region, Sustainable Fisheries Division, 7600 Sand Point Way NE., Bldg. #1, Seattle, WA 98115.

Assistant Regional Administrator and Tuna Dolphin Policy Analyst, NMFS Southwest Region, 501 West Ocean Boulevard, Suite 4200, Long Beach, CA 90802.

Information/Permit Specialist, Sustainable Fisheries Division, NMFS Pacific Islands Region, 1601 Kapiolani Boulevard, Suite 1110, Honolulu, HI 96814.

Regional Administrator, NMFS Alaska Region, 709 West Ninth Street, Juneau, AK 99801.

High Seas Fishing Compliance Act: Fishery Management Specialist, Office of International Affairs (F/IA), NMFS, 1315 East-West Highway, Room 12604, Silver Spring, MD 20910.

AMLR harvesting permits: Foreign Affairs Specialist for International Science, NMFS Office of Science and Technology, 1315 East-West Highway, Room 12350, Silver Spring, MD 20910.

AMLR dealer permits: Import Control Officer, NMFS Office of Sustainable

Fisheries, P.O. Drawer 1207, Pascagoula, MS 39567.

National Saltwater Angler Registry: Fish Biologist, Office of Science and Technology, Fisheries Statistics Division NMFS, 1315 East-West Highway, Room 12423, Silver Spring, MD 20910.

NOTIFICATION PROCEDURE:

Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the national or regional Privacy Act Officer:

Privacy Act Officer, NOAA, 1315 East-West Highway, Room 10641, Silver Spring, MD 20910.

Privacy Act Officer, NMFS, 1315 East-West Highway, Room 13706, Silver Spring, MD 20910.

Privacy Act Officer, NMFS Northeast Region, One Blackburn Drive, Gloucester, MA 01930.

Privacy Act Officer, NMFS Southeast Region, 263 13th Avenue South, St. Petersburg, FL 33701.

Privacy Act Officer, NMFS Northwest Region, 7600 Sand Point Way NE., Bldg. #1, Seattle, WA 98115.

Privacy Act Officer, NMFS Southwest Region, 501 West Ocean Boulevard, Suite 4200, Long Beach, CA 90802.

Privacy Act Officer, NMFS Pacific Islands Region, 1601 Kapiolani Boulevard, Suite 1110, Honolulu, HI 96814.

Privacy Act Officer, NMFS Alaska Region, P.O. Box 21668, Juneau, AK 99802, or delivered to the Federal Building, 709 West 9th Street, Juneau, AK 99801.

Written requests must be signed by the requesting individual. Requestor must make the request in writing and provide his/her name, address, and date of the request and record sought. All such requests must comply with the inquiry provisions of the Department's Privacy Act rules which appear at 15 CFR part 4, Appendix A.

RECORD ACCESS PROCEDURES:

Requests for access to records maintained in this system of records should be addressed to the same address given in the Notification section above. **Note:** Complete records for jointly owned permits are made accessible to each owner upon his/her request.

CONTESTING RECORD PROCEDURES:

The Department's rules for access, for contesting contents, and appealing initial determinations by the individual concerned are provided for in 15 CFR part 4, Appendix A.

RECORD SOURCE CATEGORIES:

Information in this system will be collected from individuals applying for a permit or registration or from an entity supplying related documentation regarding an application, permit, or registration.

EXEMPTION CLAIMS FOR SYSTEM:

None.

Dated: April 11, 2008.

Brenda Dolan,

Department of Commerce, Freedom of Information/Privacy Act Officer.

[FR Doc. E8–8257 Filed 4–16–08; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XH25

Taking and Importing Marine Mammals; Navy Training and Research, Development, Testing, and Evaluation Activities Conducted Within the Southern California Range Complex

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice; receipt of application for letter of authorization; request for comments and information.

SUMMARY: NMFS has received a request from the U.S. Navy (Navy) for authorization to take marine mammals incidental to military readiness training events and research, development, testing and evaluation (RDT&E) to be conducted in the Southern California Range Complex (SOCAL) for the period beginning January 2009 and ending January 2014. Pursuant to the implementing regulations of the Marine Mammal Protection Act (MMPA), NMFS is announcing our receipt of the Navy's request for the development and implementation of regulations governing the incidental taking of marine mammals and inviting information, suggestions, and comments on the Navy's application and request.

DATES: Comments and information must be received no later than May 19, 2008.

ADDRESSES: Comments on the application should be addressed to Michael Payne, Chief, Permits, Conservation and Education Division, Office of Protected Resources, National Marine Fisheries Service, 1315 East-West Highway, Silver Spring, MD 20910–3225. The mailbox address for providing email comments is *PR1.050107L@noaa.gov*. NMFS is not responsible for e-mail comments sent to addresses other than the one provided here. Comments sent via e-mail, including all attachments, must not exceed a 10–megabyte file size.

FOR FURTHER INFORMATION CONTACT: Jolie Harrison, Office of Protected Resources, NMFS, (301) 713–2289, ext. 166.

SUPPLEMENTARY INFORMATION:

Availability

A copy of the Navy's application may be obtained by writing to the address specified above (See **ADDRESSES**), telephoning the contact listed above (see **FOR FURTHER INFORMATION CONTACT**), or visiting the internet at: *http://www.nmfs.noaa.gov/pr/permits/incidental.htm*. The Navy's Draft Environmental Impact Statement (DEIS) for SOCAL was made available to the public on April 4, 2008, and may be viewed at *http://www.socalrangecomplexeis.com/*. Because NMFS is participating as a cooperating agency in the development of the Navy's DEIS for SOCAL, NMFS staff will be present at the associated public meetings and prepared to discuss NMFS' participation in the development of the EIS as well as the MMPA process for the issuance of incidental take authorizations. The dates and times of the public meetings may be viewed at: *http://www.socalrangecomplexeis.com/*.

Background

In the case of military readiness activities, sections 101(a)(5)(A) and (D) of the MMPA (16 U.S.C. 1361 *et seq.*) direct the Secretary of Commerce (Secretary) to allow, upon request, the incidental, but not intentional taking of marine mammals by U.S. citizens who engage in a specified activity (other than commercial fishing) if certain findings are made and regulations are issued or, if the taking is limited to harassment, notice of a proposed authorization is provided to the public for review.

Authorization for incidental takings may be granted if NMFS finds that the taking will have no more than a negligible impact on the species or stock(s), will not have an unmitigable adverse impact on the availability of the species or stock(s) for subsistence uses, and that the permissible methods of taking and requirements pertaining to the mitigation, monitoring and reporting of such taking are set forth.

NMFS has defined ''negligible impact'' in 50 CFR 216.103 as:

an impact resulting from the specified activity that cannot be reasonably expected to, and is not reasonably likely to, adversely

CIRCULAR NO. A-130

Revised, (Transmittal Memorandum No. 4)

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES SUBJECT: Management of Federal

Information Resources

1. **Purpose:** This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.

2. **Rescissions:** This Circular rescinds OMB Memoranda M-96-20, [A]Implementation of the Information Technology Management Reform Act of 1996;[@] M-97-02, [A]Funding Information Systems Investments;[@] M-97-09, [A]Interagency Support for Information Technology;[@] M-97-15, [A]Local Telecommunications Services Policy;[@] M-97-16, "Information Technology Architectures[@].

3. **Authorities:** OMB issues this Circular pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); the Clinger-Cohen Act (also known as Information Technology Management Reform Act of 1996[@]) (Pub. L. 104-106, Division E); the Privacy Act, as amended (5 U.S.C. 552a); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); the Federal Property and Administrative Services Act, as amended (40 U.S.C. 487); the Computer Security Act of 1987 (Pub. L. 100-235); the Budget and Accounting Act, as amended (31 U.S.C. Chapter 11); the Government Performance and Results Act of 1993(GPRA); the Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7); the Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII), Executive Order No. 12046 of March 27, 1978; Executive Order No. 12472 of April 3, 1984; and Executive Order No. 13011 of July 17, 1996.

4. Applicability and Scope:

a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal government.

b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background: The Clinger-Cohen Act supplements the information resources management policies contained in the PRA by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by:

1. focusing information resource planning to support their strategic missions;
2. implementing a capital planning and investment control process that links to budget formulation and execution; and
3. rethinking and restructuring the way they do their work before investing in information systems.

The PRA establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the PRA requires that the Director of OMB develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

6. Definitions:

a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration.

b. The term "audiovisual production" means a unified presentation, developed according to a plan or script, containing visual imagery, sound or both, and used to convey information.

c. The term "capital planning and investment control process " means a management process for ongoing identification, selection, control, and evaluation of investments in information
resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

d. The term "Chief Information Officers Council" (CIO Council) means the Council established in Section 3 of Executive Order 13011.

e. The term "dissemination" means the government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act.

f. The term "executive agency" has the meaning defined in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

g. The term "full costs," when applied to the expenses incurred in the operation of an information processing service organization (IPSO), is comprised of all direct, indirect, general, and administrative costs incurred in the operation of an IPSO. These costs include, but are not limited to, personnel, equipment, software, supplies, contracted services from private sector providers, space occupancy, intra-agency services from within the agency, inter-agency services from other Federal agencies, other services that are provided by State and local governments, and Judicial and Legislative branch organizations.

h. The term "government information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

i. The term "government publication" means information which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)

j. The term "information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

k. The term "information dissemination product" means any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.

l. The term "information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

m. The term "information management" means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

n. The term "information resources" includes both government information and information technology.

o. The term "information processing services organization" (IPSO) means a discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.

p. The term "information resources management" means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

q. The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

r. The term "information system life cycle" means the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

s. The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

t. The term "Information Technology Resources Board" (Resources Board) means the board established by Section 5 of Executive Order 13011.

u. The term "major information system" means an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

v. The term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be administrative and business applications (including payroll, finance, logistics, and personnel management applications). The policies and procedures established in this Circular will apply to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in Section 5141 of the Clinger-Cohen Act (Pub. L. 104-106, 40 U.S.C. 1451). Applicability of Clinger-Cohen Act to national security systems shall include budget document preparation requirements set forth in OMB Circular A-11. The resultant budget document may be classified in accordance with the provisions of Executive Order 12958.

w. The term "records" means all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received
by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

x. The term "records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

y. The term "service recipient" means an agency organizational unit, programmatic entity, or chargeable account that receives information processing services from an information processing service organization (IPSO). A service recipient may be either internal or external to the organization responsible for providing information resources services, but normally does not report either to the manager or director of the IPSO or to the same immediate supervisor.

7. Basic Considerations and Assumptions:

a. The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States. Because of the extent of the government's information activities, and the dependence of those activities upon public cooperation, the management of Federal information resources is an issue of continuing importance to all Federal agencies, State and local governments, and the public.

b. Government information is a valuable national resource. It provides the public with knowledge

of the government, society, and economy -- past, present, and future. It is a means to ensure the accountability of government, to manage the government's operations, to maintain the healthy performance of the economy, and is itself a commodity in the marketplace.

c. The free flow of information between the government and the public is essential to a democratic society. It is also essential that the government minimize the Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information, the expected public and private benefits derived from government information should exceed the public and private costs of the information, recognizing that the benefits to be derived from government information may not always be quantifiable.

e. The nation can benefit from government information disseminated both by Federal agencies and by diverse nonfederal parties, including State and local government agencies, educational and other not-for-profit institutions, and for-profit organizations..

f. Because the public disclosure of government information is essential to the operation of a democracy, the management of Federal information resources should protect the public's right of access to government information.

g. The individual's right to privacy must be protected in Federal Government information activities involving personal information.

h. Systematic attention to the management of government records is an essential component of sound public resources management which ensures public accountability. Together with records preservation, it protects the government's historical record and guards the legal and financial rights of the government and the public.

i. Strategic planning improves the operation of government programs. The agency strategic plan will shape the redesign of work processes and guide the development and maintenance of an Enterprise Architecture and a capital planning and investment control process. This management approach promotes the appropriate application of Federal information resources

j. Because State and local governments are important producers of government information for many areas such as health, social welfare, labor, transportation, and education, the Federal Government must cooperate with these governments in the management of information resources.

k. The open and efficient exchange of scientific and technical government information, subject to applicable national security controls and the proprietary rights of others, fosters excellence in scientific research and effective use of Federal research and development funds.

l. Information technology is not an end in itself. It is one set of resources that can improve the effectiveness and efficiency of Federal program delivery.

m. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

n. Users of Federal information resources must have skills, knowledge, and training to manage information resources, enabling the Federal government to effectively serve the public through automated means.

o. The application of up-to-date information technology presents opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

p. The availability of government information in diverse media, including electronic formats, permits agencies and the public greater flexibility in using the information.

q. Federal managers with program delivery responsibilities should recognize the importance of information resources management to mission performance.

r. The Chief Information Officers Council and the Information Technology Resources Board will help in the development and operation of interagency and interoperable shared information resources to support the performance of government missions.

8. Policy:

a. Information Management Policy

1. How will agencies conduct Information Management Planning?

Agencies must plan in an integrated manner for managing information throughout its life cycle. Agencies will:

(a) Consider, at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle, particularly those concerning information dissemination;

(b) Consider the effects of their actions on members of the public and ensure consultation with the public as appropriate;

(c) Consider the effects of their actions on State and local governments and ensure consultation with those governments as appropriate;

(d) Seek to satisfy new information needs through interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(e) Integrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition, and use of information technology;

(f) Train personnel in skills appropriate to management of information;

(g) Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information;

(h) Use voluntary standards and Federal Information Processing Standards where appropriate or required;

(i) Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented;

(j) Record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government;

(k) Incorporate records management and archival functions into the design, development, and implementation of information systems;

1. Provide for public access to records where required or appropriate.

2. What are the guidelines for Information Collection?

Agencies must collect or create only that information necessary for the proper performance of agency functions and which has practical utility.

3. What are the guidelines for Electronic Information Collection?
Executive agencies under Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII, are required to provide, by October 21, 2003, the (1) option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and (2) use and acceptance of electronic signatures, when practicable. Agencies will follow the provisions in OMB Memorandum M-00-10, Procedures and Guidance on Implementing of the Government Paperwork Elimination Act.[@]

4. How must agencies implement Records Management? Agencies will:

(a) Ensure that records management programs provide adequate and proper documentation of agency activities;

(b) Ensure the ability to access records regardless of form or medium;

(c) In a timely fashion, establish, and obtain the approval of the Archivist of the United States for retention schedules for Federal records; and

(d) Provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities.

5. How must an agency provide information to the public?
Agencies have a responsibility to provide information to the public consistent with their missions. Agencies will discharge this responsibility by:

(a) Providing information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;

(b) Providing access to agency records under provisions of the Freedom of Information Act and the Privacy Act, subject to the protections and limitations provided for in these Acts;

(c) Providing such other information as is necessary or appropriate for the proper performance of agency functions; and

(d) In determining whether and how to disseminate information to the public, agencies will:

(i) Disseminate information in a manner that achieves the best balance between the goals of maximizing the usefulness of the information and minimizing the cost to the government and the public;

(ii) Disseminate information dissemination products on equitable and timely terms;

(iii) Take advantage of all dissemination channels, Federal and nonfederal, including State and local governments, libraries and

private sector entities, in discharging agency information dissemination responsibilities;

(iv) Help the public locate government information maintained by or for the agency.

6. What is an Information Dissemination Management System?
Agencies will maintain and implement a management system for all information dissemination products which must, at a minimum:

(a) Assure that information dissemination products are necessary for proper performance of agency functions (44 U.S.C. 1108);

(b) Consider whether an information dissemination product available from other Federal or nonfederal sources is equivalent to an agency information dissemination product and reasonably fulfills the dissemination responsibilities of the agency;

(c) Establish and maintain inventories of all agency information dissemination products;

(d) Develop such other aids to locating agency information dissemination products including catalogs and directories, as may reasonably achieve agency information dissemination objectives;

(e) Identify in information dissemination products the source of the information, if from another agency;

(f) Ensure that members of the public with disabilities whom the agency has a responsibility to inform have a reasonable ability to access the information dissemination products;

(g) Ensure that government publications are made available to depository libraries through the facilities of the Government Printing Office, as required by law (44 U.S.C. Part 19);

(h) Provide electronic information dissemination products to the Government Printing Office for distribution to depository libraries;

(i) Establish and maintain communications with members of the public and with State and local governments so that the agency creates information dissemination products that meet their respective needs;

(j) Provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and

(k) Ensure that, to the extent existing information dissemination policies or practices are inconsistent with the requirements of this Circular, a prompt and orderly transition to compliance with the requirements of this Circular is made.

7. How must agencies avoid improperly restrictive practices? Agencies will:

(a) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the availability of information dissemination products on a timely and equitable basis;

(b) Avoid establishing restrictions or regulations, including the charging of fees or royalties, on the reuse, resale, or redissemination of Federal information dissemination products by the public; and,

(c) Set user charges for information dissemination products at a level sufficient to recover the cost of dissemination but no higher. They must exclude from calculation of the charges costs associated with original collection and processing of the information. Exceptions to this policy are:

(i) Where statutory requirements are at variance with the policy;

(ii) Where the agency collects, processes, and disseminates the information for the benefit of a specific identifiable group beyond the benefit to the general public;

(iii) Where the agency plans to establish user charges at less than cost of dissemination because of a determination that higher charges would constitute a significant barrier to properly performing the agency's functions, including reaching members of the public whom the agency has a responsibility to inform; or

(iv) Where the Director of OMB determines an exception is warranted.

8. How will agencies carry out electronic information dissemination?
Agencies will use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make government information more easily accessible and useful to the public. The use of electronic media and formats for information dissemination is appropriate under the following conditions:

(a) The agency develops and maintains the information electronically;

(b) Electronic media or formats are practical and cost effective ways to provide public access to a large, highly detailed volume of information;

(c) The agency disseminates the product frequently;

(d) The agency knows a substantial portion of users have ready access to the necessary information technology and training to use electronic information dissemination products;

(e) A change to electronic dissemination, as the sole means of disseminating the product, will not impose substantial acquisition or training costs on users, especially State and local governments and small business entities.

9. What safeguards must agencies follow? Agencies will:

(a) Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or

unauthorized access to or modification of such information;

(b) Limit the collection of information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions;

(c) Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;

(d) Provide individuals, upon request, access to records about them maintained in Privacy Act systems of records, and permit them to amend such records as are in error consistent with the provisions of the Privacy Act.

b. How Will Agencies Manage Information Systems and Information Technology?

(1) How will agencies use capital planning and investment control process?

Agencies must establish and maintain a capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner. The process will guide both strategic and operational IRM, IT planning, and the Enterprise Architecture by integrating the agency's IRM plans, strategic and performance plans prepared pursuant to the Government Performance and Results Act of 1993, financial management plans prepared pursuant to the Chief Financial Officer Act of 1990 (31 U. S.C. 902a5), acquisition under the Federal Acquisition Streamlining Act of 1994, and the agency's budget formulation and execution processes. The capital planning and investment control process includes all stages of capital programming, including planning, budgeting, procurement, management, and assessment.

As outlined below, the capital planning and investment control process has three components: selection, control, and evaluation. The process must be iterative, with inputs coming from all of the agency plans and the outputs feeding into the budget and investment control processes. The goal is to link resources to results (for further guidance on Capital Planning refer to OMB Circular A-11). The agency's capital planning and investment control process must build from the agency's current Enterprise Architecture (EA) and its transition from current architecture to target architecture. The Capital Planning and Investment Control processes must be documented, and provided to OMB consistent with the budget process. The Enterprise Architecture must be documented and provided to OMB as significant changes are incorporated.

(a) What plans are associated with the capital planning and investment control process?

In the capital planning and investment control process, there are two separate and distinct plans that address IRM and IT planning requirements for the agency. The IRM Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency Information Resource Management Strategic Plan (IRM) as required by 44 U.S.C. 3506 (b) (2). IRM Strategic Plans should support the agency Strategic Plan required in OMB Circular A-11, provide a description of how information resources management activities help accomplish agency missions, and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

The IT Capital Plan is operational in nature, supports the goals and missions identified in the IRM Strategic Plan, is a living document, and must be updated twice yearly. This IT Capital Plan is the implementation plan for the budget year. The IT Capital Plan should also reflect the goals of the agency's Annual Performance Plan, the agency's Government Paperwork Elimination Act (GPEA) Plan, the agency's EA, and agency's business planning processes. The IT Capital Plan must be submitted annually to OMB with the agency budget submission. annually. The IT Capital Plan must include the following components:

(i) A component, derived from the agency's capital planning and investment control process under OMB Circular A-11, Section 300 and the OMB Capital Programming Guide, that specifically includes all IT Capital Asset Plans for major information systems or projects. This component must also demonstrate how the agency manages its other IT investments, as required by the Clinger-Cohen Act.

(ii) A component that addresses two other sections of OMB Circular A-11: a section for Information on Financial Management, including the Report on Financial Management Activities and the Agency=s Financial Management Plan, and a section entitled Information Technology, including the Agency IT Investment Portfolio.

(iii) A component, derived from the agency=s capital planning and investment control process, that demonstrates the criteria it will use to select the investments into the portfolio, how it will control and manage the investments, and how it will evaluate the investments based on planned performance versus actual accomplishments.

(iv) A component that includes a summary of the security plan from the agency's five-year plan as required by the PRA and Appendix III of this Circular. The plan must demonstrate that IT projects and the EA include security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from National Institute of Standards and Technology (NIST) security guidance.

(b) What must an agency do as part of the selection component of the capital planning process? It must:

(i) Evaluate each investment in information resources to determine whether the investment will support core mission functions that must be performed by the Federal government;

(ii) Ensure that decisions to improve existing information systems or develop new information systems are initiated only when no alternative private sector or governmental source can efficiently meet the need;

(iii) Support work processes that it has simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial, off-the-shelf technology;

(iv) Reduce risk by avoiding or isolating custom designed components, using components that can be fully tested or prototyped prior to production, and ensuring involvement and support of users;

(v) Demonstrate a projected return on the investment that is clearly equal to or better than alternative uses of available public resources. The return may include improved mission performance in accordance with GPRA measures, reduced cost, increased quality, speed, or flexibility; as well as increased customer and employee satisfaction. The return should reflect such risk factors as the project's technical complexity, the agency's management capacity, the likelihood of cost overruns, and the consequences of under- or non-performance. Return on investment should, where appropriate, reflect actual returns observed through pilot projects and prototypes;

(vi) Prepare and update a benefit-cost analysis (BCA) for each information system throughout its life cycle. A BCA will provide a level of detail proportionate to the size of the investment, rely on systematic measures of mission performance, and be consistent with the methodology described in OMB Circular No. A-94, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs";

(vii) Prepare and maintain a portfolio of major information systems that monitors investments and prevents redundancy of existing or shared IT capabilities. The portfolio will provide information demonstrating the impact of alternative IT investment strategies and funding levels, identify opportunities for sharing resources, and consider the agency's inventory of information resources;

(viii) Ensure consistency with Federal, agency, and bureau Enterprise architectures, demonstrating such consistency through compliance with agency business requirements and standards, as well as identification of milestones, as defined in the EA;

(ix) Ensure that improvements to existing information systems and the development of planned information systems do not unnecessarily duplicate IT capabilities within the same agency, from other agencies, or from the private sector;

(x) Ensure that the selected system or process maximizes the usefulness of information, minimizes the burden on the public, and preserves the appropriate integrity, usability, availability, and confidentiality of information throughout the life cycle of the information, as determined in accordance with the PRA and the Federal Records Act. This portion must specifically address the planning and budgeting for the information collection burden imposed on the public as defined by 5 CFR 1320;

(xi) Establish oversight mechanisms, consistent with Appendix III of this Circular, to evaluate systematically and ensure the continuing security, interoperability, and availability of systems and their data;

(xii) Ensure that Federal information system requirements do not unnecessarily restrict the prerogatives of state, local and tribal governments;

(xiii) Ensure that the selected system or process facilitates accessibility under the Rehabilitation Act of 1973, as amended.

(c) What must an agency do as part of the control component of the capital planning process? It must:

(i) Institute performance measures and management processes that monitor actual performance compared to expected results. Agencies must use a performance based management system that provides timely information regarding the progress of an information technology investment. The system must also measure progress towards milestones in an independently verifiable basis, in terms of cost, capability of the investment to meet specified requirements, timeliness, and quality;

(ii) Establish oversight mechanisms that require periodic review of information systems to determine how mission requirements might have changed, and whether the information system continues to fulfill ongoing and anticipated mission requirements. These mechanisms must also require information regarding the future levels of performance, interoperability, and maintenance necessary to ensure the information system meets mission requirements
cost effectively;

(iii) Ensure that major information systems proceed in a timely fashion towards agreed upon milestones in an information system life cycle. Information systems must also continue to deliver intended benefits to the agency and customers, meet user requirements, and identify and offer security protections;

(iv) Prepare and update a strategy that identifies and mitigates risks associated with each information system;

(iv) Ensure that financial management systems conform to the requirements of OMB Circular No. A-127, "Financial Management Systems;"

(v) Provide for the appropriate management and disposition of records in accordance with the Federal Records Act.

(vi) Ensure that agency EA procedures are being followed. This includes ensuring that EA milestones are reached and documentation is updated as needed.

(d) What must an agency do as part of the evaluation component of the capital planning process?

It must:

(i) Conduct post-implementation reviews of information systems and information resource management processes to validate estimated benefits and costs, and document effective management practices for broader use;

(ii) Evaluate systems to ensure positive return on investment and decide whether continuation, modification, or termination of the systems is necessary to meet agency mission requirements.

(iii) Document lessons learned from the post-implementation reviews. Redesign oversight mechanisms and performance levels to incorporate acquired knowledge.

(iv) Re-assess an investment's business case, technical compliance, and compliance against the EA.

(v) Update the EA and IT capital planning processes as needed. (2) The Enterprise

Architecture

Agencies must document and submit their initial EA to OMB. Agencies must submit updates when significant changes to the Enterprise Architecture occur.

(a) What is the Enterprise Architecture?

An EA is the explicit description and documentation of the current and desired relationships among business and management processes and information technology. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency¯s capital planning and investment control processes, agency EA planning processes, and agency systems life cycle

methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with GPEA, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail. Agencies must implement the EA consistent with following principles:

(i) Develop information systems that facilitate interoperability, application portability, and scalability of electronic applications across networks of heterogeneous hardware, software, and telecommunications platforms;

(ii) Meet information technology needs through cost effective intra-agency and interagency sharing, before acquiring new information technology resources; and

(iii) Establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems.

(b) How do agencies create and maintain the EA?

As part of the EA effort, agencies must use or create an Enterprise Architecture Framework. The Framework must document linkages between mission needs, information content, and information technology capabilities. The Framework must also guide both strategic and operational IRM planning.

Once a framework is established, an agency must create the EA. In the creation of an EA, agencies must identify and document:

(i) Business Processes - Agencies must identify the work performed to support its mission, vision and performance goals. Agencies must also document change agents, such as legislation or new technologies that will drive changes in the EA.

(ii) Information Flow and Relationships - Agencies must analyze the information utilized by the agency in its business processes, identifying the information used and the movement of the information. These information flows indicate where the information is needed and how the information is shared to support mission functions.

(iii) Applications - Agencies must identify, define, and organize the activities that capture, manipulate, and manage the business information to support business processes. The EA also describes the logical dependencies and relationships among business activities.

(iv) Data Descriptions and Relationships - Agencies must identify how data is created, maintained, accessed, and used. At a high level, agencies must define the data and describe the relationships among data elements used in the agency's information systems.

(v) Technology Infrastructure - Agencies must describe and identify the functional characteristics, capabilities, and interconnections of the hardware, software, and telecommunications.

(c) What are the Technical Reference Model and Standards Profile?
The EA must also include a Technical Reference Model (TRM) and Standards Profile. (i) The TRM identifies and describes the information services (such as database,
communications, intranet, etc.) used throughout the agency.

(ii) The Standards Profile defines the set of IT standards that support the services articulated in the TRM. Agencies are expected to adopt standards necessary to support the entire EA, which must be enforced consistently throughout the agency.

(iii) As part of the Standards Profile, agencies must create a Security Standards Profile that is specific to the security services specified in the EA and covers such services as identification, authentication, and non-repudiation; audit trail creation and analysis; access controls; cryptography management; virus protection; fraud prevention; detection and mitigation; and intrusion prevention and detection.

(3) How Will Agencies Ensure Security in Information Systems?

Agencies must incorporate security into the architecture of their information and systems to ensure that security supports agency business operations and that plans to fund and manage security are built into life-cycle budgets for information systems.

(a) To support more effective agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:

(i) Prioritize key systems (including those that are most critical to agency operations);

(ii) Apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of harm;

(b) Agencies must make security¯s role explicit in information technology investments and capital programming. Investments in the development of new or the continued operation of existing information systems, both general support systems and major applications must:

(i) Demonstrate that the security controls for components, applications, and systems are consistent with, and an integral part of, the EA of the agency;

(ii) Demonstrate that the costs of security controls are understood and are explicitly incorporated into the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming;

(iii) Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;

(iv) Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time;

(v) Demonstrate specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages;

(vi) Identify additional security controls that are necessary to minimize risk to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control;

(vii) Deploy effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access;

(viii) Ensure that the handling of personal information is consistent with relevant government-wide and agency policies;

(ix) Describe each occasion the agency decides to employ standards and guidance that are more stringent than those promulgated by NIST to ensure the use of risk-based costeffective security controls for non-national security applications;

(c) OMB will consider for new or continued funding only those system investments that satisfy these criteria. New information technology investments must demonstrate that existing agency systems also meet these criteria in order to qualify for funding.

(4) How Will Agencies Acquire Information Technology? Agencies must:

(a) Make use of adequate competition, allocate risk between government and contractor, and maximize return on investment when acquiring information technology;

(b) Structure major information systems into useful segments with a narrow scope and brief duration. This should reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions;

(c) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software is clear and has been documented through pilot projects or prototypes; and

(d) Ensure accessibility of acquired information technology pursuant to the Rehabilitation Act of 1973, as amended (Pub. Law 105-220, 29 U.S.C.794d).

9. Assignment of Responsibilities:

a. All Federal Agencies. The head of each agency must:

1. Have primary responsibility for managing agency information resources;

2. Ensure that the agency implements appropriately all of the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB;

3. Appoint a Chief Information Officer, as required by 44 U.S.C. 3506(a), who must report directly to the agency head to carry out the responsibilities of the agencies listed in the Paperwork Reduction Act (44 U.S.C. 3506), the Clinger Cohen Act (40 U.S.C. 1425(b) & (c)), as well as Executive Order 13011. The head of the agency must consult with the Director of OMB prior to appointing a Chief Information Officer, and will advise the Director on matters regarding the authority, responsibilities, and organizational resources of the Chief Information Officer. For purposes of this paragraph, military departments and the Office of the Secretary of Defense may each appoint one official. The Chief Information Officer must, among other things:

(a) Be an active participant during all agency strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans;

(b) Advise the agency head on information resource implications of strategic planning decisions;

(c) Advise the agency head on the design, development, and implementation of information resources.

(i) Monitor and evaluate the performance of information resource investments through a capital planning and investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project;

(ii) Advise the agency head on budgetary implications of information resource decisions; and

(d) Be an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources;

4. Direct the Chief Information Officer to monitor agency compliance with the policies, procedures, and guidance in this Circular. Acting as an ombudsman, the Chief Information Officer must consider alleged instances of agency failure to comply with this Circular, and recommend or take appropriate corrective action. The Chief Information Officer will report instances of alleged failure and their resolution annually to the Director of OMB, by February 1 st of each year.

5. Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

6. Develop agency policies and procedures that provide for timely acquisition of required information technology;

7. Maintain the following, as required by the Paperwork Reduction Act (44 U.S.C. 3506(b)(4) and 3511) and the Freedom of Information Act (5 U.S.C. 552(g)): an inventory of the agency=s major information systems, holdings, and dissemination products; an agency information locator service; a description of the agency=s major information and record locator systems; an inventory of the agency=s other information resources, such as personnel and funding (at the level of detail that the agency determines is most appropriate for its use in managing the agency=s information resources); and a handbook for persons to obtain public information from the agency pursuant to these Acts.

8. Implement and enforce applicable records management policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.

9. Identify to the Director of OMB any statutory, regulatory, and other impediments to efficient management of Federal information resources, and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

10. Assist OMB in the performance of its functions under the PRA, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

11. Ensure that the agency:

(a) cooperates with other agencies in the use of information technology to improve the productivity, effectiveness, and efficiency of Federal programs;

(b) promotes a coordinated, interoperable, secure, and shared government wide infrastructure that is provided and supported by a diversity of private sector suppliers; and

(c) develops a well-trained corps of information resource professionals.

12. Use the guidance provided in OMB Circular A-11, "Planning, Budgeting, and Acquisition of Fixed Assets," to promote effective and efficient capital planning within the organization;

13. Ensure that the agency provides budget data pertaining to information resources to OMB, consistent with the requirements of OMB Circular A-11,

14. Ensure, to the extent reasonable, that in the design of information systems with the purpose of disseminating information to the public, an index of information disseminated by the system will be included in the directory created by the Superintendent of Documents pursuant to 41 U.S.C. 4101. (Nothing in this paragraph authorizes the dissemination of information to the public unless otherwise authorized.)

15. Permit, to the extent practicable, the use of one agency's contract by another agency or the award of multi-agency contracts, provided the action is within the scope of the contract and consistent with OMB guidance; and

16. As designated by the Director of OMB, act as executive agent for the government-wide acquisition of information technology.

b. Department of State. The Secretary of State must:

1. Advise the Director of OMB on the development of United States positions and policies on international information policy and technology issues affecting Federal government activities and the development of international information technology standards; and

2. Be responsible for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to information resources management, including federal information technology. The Secretary must also ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international standards and recommendations affecting information technology. These responsibilities may also require the Secretary to consult, as appropriate, with affected domestic agencies, organizations, and other members of the public.

c. Department of Commerce. The Secretary of Commerce must:

1. Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology, while taking into consideration the recommendations of the agencies and the CIO Council;

2. Advise the Director of OMB on the development of policies relating to the procurement and management of Federal telecommunications resources;

3. Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;

4. Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems, and advise the Director of OMB and appropriate agencies of the recommendations that result from such studies;

5. Develop, in consultation with the Secretary of State and the Director of OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities;

6. Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

7. Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of State, international information technology standards, and advise the Director of OMB on such activities.

d. Department of Defense. The Secretary of Defense will develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

e. General Services Administration. The Administrator of General Services must:

1. Continue to manage the FTS2001 program and coordinate the follow-up to that program, on behalf of and with the advice of agencies;

2. Develop, maintain, and disseminate for the use of the Federal community (as requested by OMB or the agencies) recommended methods and strategies for the development and acquisition of information technology;

3. Conduct and manage outreach programs in cooperation with agency managers;

4. Be a liaison on information resources management (including Federal information technology) with State and local governments. GSA must also be a liaison with nongovernmental international organizations, subject to prior consultation with the Secretary of State to ensure consistency with the overall United States foreign policy objectives;

5. Support the activities of the Secretary of State for liaison, consultation, and negotiation with intergovernmental organizations on information resource management matters;

6. Provide support and assistance to the CIO Council and the Information Technology Resources Board.

7. Manage the Information Technology Fund in accordance with the Federal Property and Administrative Services Act, as amended;

f. Office of Personnel Management. The Director, Office of Personnel Management, will:

1. Develop and conduct training programs for Federal personnel on information resources management, including end-user computing;

2. Evaluate periodically future personnel management and staffing requirements for Federal information resources management;

3. Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States will:

1. Administer the Federal records management program in accordance with the National Archives and Records Act;

2. Assist the Director of OMB in developing standards and guidelines relating to the records management program.

h. Office of Management and Budget. The Director of the Office of Management and Budget will:

1. Provide overall leadership and coordination of Federal information resources management within the executive branch;

2. Serve as the President's principal adviser on procurement and management of Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;

3. Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;

4. Initiate and review proposals for changes in legislation, regulations, and agency procedures to improve Federal information resources management;

5. Review and approve or disapprove agency proposals for collection of information from the public, as defined by 5 CFR 1320.3;

6. Develop and maintain a Governmentwide strategic plan for information resources management.

7. Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;

8. Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration, coordinate records management policies and programs with other information activities, and review compliance by agencies with records management requirements;

9. Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance, with respect to privacy and security, with the Privacy Act, the Freedom of Information Act, the Computer Security Act, the GPEA, and related statutes;

10. Review proposed U. S. Government Position and Policy statements on international issues affecting Federal Government information activities, and advise the Secretary of State as to their consistency with Federal information resources management policy.

11. Coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy, and policies regarding management of financial management systems with the Office of Federal Financial Management.

12. Evaluate agency information resources management practices and programs and, as part of the budget process, oversee agency capital planning and investment control processes to analyze, track, and evaluate the risks and results of major capital investments in information systems;

13. Notify an agency if OMB believes that a major information system project requires outside assistance;

14. Provide guidance on the implementation of the Clinger-Cohen Act and on the management of information resources to the executive agencies, to the CIO Council, and to the Information Technology Resources Board; and

15. Designate one or more heads of executive agencies as executive agent for governmentwide acquisitions of information technology.

10. Oversight:

a. The Director of OMB will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

b. The Director of OMB may, consistent with statute and upon written request of an agency, grant a waiver from particular requirements of this Circular. Requests for waivers must detail the reasons why a particular waiver is sought, identify the duration of the waiver sought, and include a plan for the prompt and orderly transition to full compliance with the requirements of this Circular. Notice of each waiver request must be published promptly by the agency in the Federal Register, with a copy of the waiver request made available to the public on request.

11. **Effectiveness:** This Circular is effective upon issuance. Nothing in this Circular will be construed to confer a private right of action on any person.

12. **Inquiries:** All questions or inquiries should be addressed to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3785.

13. **Sunset Review Date:** OMB will review this Circular three years from the date of issuance to ascertain its effectiveness.

NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

Marianne Swanson
Joan Hash
Pauline Bowen

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

Reports on Information Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology promotes the United States economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national-security-related information in federal information systems. This Special Publication 800 series reports on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgements

The National Institute of Standards and Technology would like to acknowledge the authors of the original NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology System.* The original document was used as the foundation for this revision. Additionally, thank you to all the NIST staff that reviewed and commented on the document.

Table of Contents

Executive Summary

The objective of system security planning is to improve protection of information system resources. All federal systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and" Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA).

The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the senior agency information security officer (SAISO). Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

In order for the plans to adequately reflect the protection of the resources, a senior management official must authorize a system to operate. The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, the manager accepts its associated risk.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the system security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by the assessment report and the plan of actions and milestones. In addition, a periodic review of controls should also contribute to future authorizations. Re-authorization should occur whenever there is a significant change in processing, but at least every three years.

1. Introduction

Today's rapidly changing technical environment requires federal agencies to adopt a minimum set of security controls to protect their information and information systems. Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies the minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements defined in FIPS 200 through the use of the security controls in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*. NIST SP 800-53 contains the management, operational, and technical safeguards or countermeasures prescribed for an information system. The controls selected or planned must be documented in a system security plan. This document provides guidance for federal agencies for developing system security plans for federal information systems.

1.1 Background

Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), requires each federal agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. System security planning is an important activity that supports the system development life cycle (SDLC) and should be updated as system events trigger the need for revision in order to accurately reflect the most current state of the system. The system security plan provides a summary of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan also may reference other key security-related documents for the information system such as a risk assessment, plan of action and milestones, accreditation decision letter, privacy impact assessment, contingency plan, configuration management plan, security configuration checklists, and system interconnection agreements as appropriate.

1.2 Target Audience

Program managers, system owners, and security personnel in the organization must understand the system security planning process. In addition, users of the information system and those responsible for defining system requirements should be familiar with the system security planning process. Those responsible for implementing and managing information systems must participate in addressing security controls to be applied to their systems. This guidance provides basic information on how to prepare a system security plan and is designed to be adaptable in a variety of organizational structures and used as reference by those having assigned responsibility for activity related to security planning.

1.3 Organization of Document

This publication introduces a set of activities and concepts to develop an information system security plan. A brief description of its contents follows:

- ***Chapter 1*** includes background information relevant to the system security planning process, target audience, information on FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, a discussion of the various categories of information systems, identification of related NIST publications, and a description of the roles and responsibilities related to the development of system security plans.
- ***Chapter 2*** discusses how agencies should analyze their information system inventories in the process of establishing system boundaries. It also discusses identification of common security controls and scoping guidance.
- ***Chapter 3*** takes the reader through the steps of system security plan development.
- ***Appendix A*** provides a system security plan template.
- ***Appendix B*** provides a glossary of terms and definitions.
- ***Appendix C*** includes references that support this publication.

1.4 Systems Inventory and Federal Information Processing Standards (FIPS 199)

FISMA requires that agencies have in place an information systems inventory. All information systems in the inventory should be categorized using FIPS 199 as a first step in the system security planning activity.

FIPS 199 is the mandatory standard to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to impact. Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (i) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (ii) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

1.5 Major Applications, General Support Systems, and Minor Applications

All information systems must be covered by a system security plan and labeled as a major application[1] or general support system.[2] Specific system security plans for minor

[1] OMB Circular A-130, Appendix III, defines major application as an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

[2] OMB Circular A-130, Appendix III, defines general support system as an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.

applications[3] are not required because the security controls for those applications are typically provided by the general support system or major application in which they operate. In those cases where the minor application is not connected to a major application or general support system, the minor application should be briefly described in a general support system plan that has either a common physical location or is supported by the same organization. Additional information is provided in Chapter 2.

1.6 Other Related NIST Publications

In order to develop the system security plan, it is necessary to be familiar with NIST security standards and guidelines. It is essential that users of this publication understand the requirements and methodology for information system categorization as described in NIST FIPS 199 as well as the requirements for addressing minimum security controls for a given system as described in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* and FIPS 200*, Minimum Security Requirements for Federal information and Information System.*

Other key NIST publications directly supporting the preparation of the security plan are NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* and NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.* All documents can be obtained from the NIST Computer Security Resource Center website at: http://csrc.nist.gov/.

1.7 System Security Plan Responsibilities

Agencies should develop policy on the system security planning process. System security plans are living documents that require periodic review, modification, and plans of action and milestones for implementing security controls. Procedures should be in place outlining who reviews the plans, keeps the plan current, and follows up on planned security controls. In addition, procedures should require that system security plans be developed and reviewed prior to proceeding with the security certification and accreditation process for the system.

During the security certification and accreditation process, the system security plan is analyzed, updated, and accepted. The certification agent confirms that the security controls described in the system security plan are consistent with the FIPS 199 security category determined for the information system, and that the threat and vulnerability identification and initial risk determination are identified and documented in the system security plan, risk assessment, or equivalent document. The results of a security certification are used to reassess the risks, develop the plan of action and milestones (POA&Ms) which are required to track remedial actions, and update the system security plan, thus providing the factual basis for an authorizing official to render a security

[3] NIST Special Publication 800-37 defines a minor application as an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

accreditation decision. For additional information on the certification and accreditation process, see NIST SP 800-37. Figure 1, depicts the key inputs/outputs into the security planning process.

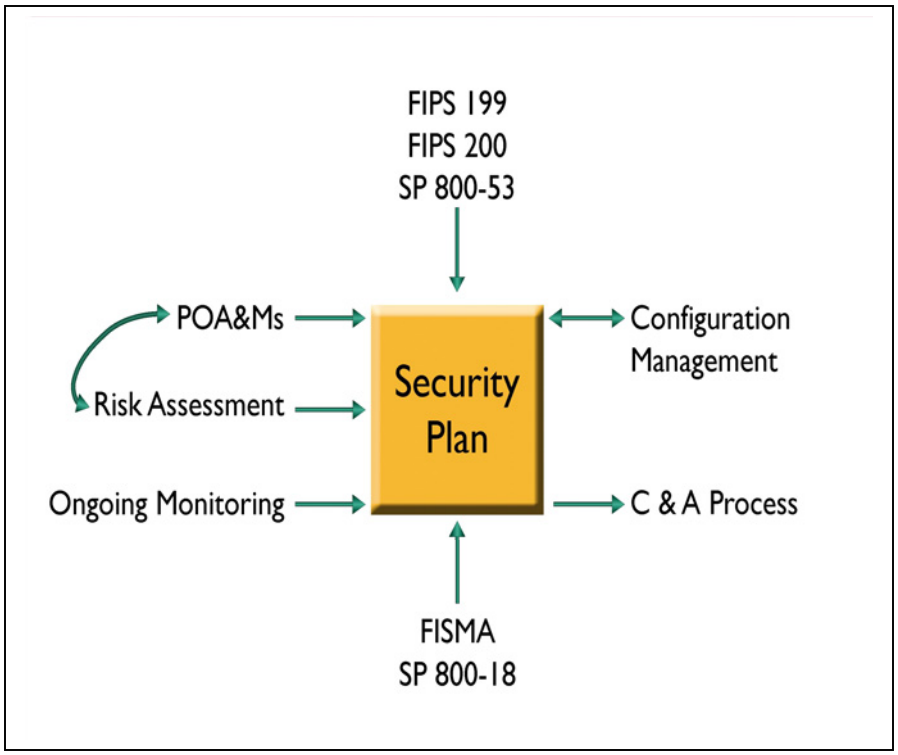


Figure 1: Security Planning Process Inputs/Outputs

The roles and responsibilities in this section are specific to information system security planning. Recognizing that agencies have widely varying missions and organizational structures, there may be differences in naming conventions for security planning-related roles and how the associated responsibilities are allocated among agency personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles[4]).

1.7.1 Chief Information Officer

The Chief Information Officer (CIO)[5] is the agency official responsible for developing and maintaining an agency-wide information security program and has the following responsibilities for system security planning:

- Designates a senior agency information security officer (SAISO) who shall carry out the CIO's responsibilities for system security planning,

[4] Caution should be exercised when one individual fills multiple roles in the security planning process to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest.

[5] When an agency has not designated a formal CIO position, FISMA requires the associated responsibilities to be handled by a comparable agency official.

- Develops and maintains information security policies, procedures, and control techniques to address system security planning,

- Manages the identification, implementation, and assessment of common security controls,

- Ensures that personnel with significant responsibilities for system security plans are trained,

- Assists senior agency officials with their responsibilities for system security plans, and

- Identifies and coordinates common security controls for the agency.

1.7.2 Information System Owner

The information system owner[6] is the agency official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. The information system owner has the following responsibilities related to system security plans:

- Develops the system security plan in coordination with information owners, the system administrator, the information system security officer, the senior agency information security officer, and functional "end users,"

- Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements,

- Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior),

- Updates the system security plan whenever a significant change occurs, and

- Assists in the identification, implementation, and assessment of the common security controls.

1.7.3 Information Owner

The information owner is the agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The information owner has the following responsibilities related to system security plans:

[6] The role of the information system owner can be interpreted in a variety of ways depending on the particular agency and the system development life cycle phase of the information system. Some agencies may refer to information system owners as program managers or business/asset/mission owners.

- Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),[7]

- Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides,

- Decides who has access to the information system and with what types of privileges or access rights, and

- Assists in the identification and assessment of the common security controls where the information resides.

1.7.4 Senior Agency Information Security Officer (SAISO)

The senior agency information security officer is the agency official responsible for serving as the CIO's primary liaison to the agency's information system owners and information system security officers. The SAISO has the following responsibilities related to system security plans:

- Carries out the CIO's responsibilities for system security planning,

- Coordinates the development, review, and acceptance of system security plans with information system owners, information system security officers, and the authorizing official,

- Coordinates the identification, implementation, and assessment of the common security controls, and

- Possesses professional qualifications, including training and experience, required to develop and review system security plans.

1.7.5 Information System Security Officer

The information system security officer is the agency official assigned responsibility by the SAISO, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program. The information system security officer has the following responsibilities related to system security plans:

- Assists the senior agency information security officer in the identification, implementation, and assessment of the common security controls, and

[7] The information owner retains that responsibility even when the data/information are shared with other organizations.

- Plays an active role in developing and updating the system security plan as well as coordinating with the information system owner any changes to the system and assessing the security impact of those changes.

1.7.6 Authorizing Official

The authorizing official (or designated approving/accrediting authority as referred to by some agencies) is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.[8] The authorizing official has the following responsibilities related to system security plans:

- Approves system security plans,
- Authorizes operation of an information system,
- Issues an interim authorization to operate the information system under specific terms and conditions, or
- Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

1.8 Rules of Behavior

The rules of behavior, which are required in OMB Circular A-130, Appendix III, and is a security control contained in NIST SP 800-53, should clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules should state the consequences of inconsistent behavior or noncompliance and be made available to every user prior to receiving authorization for access to the system. It is required that the rules contain a signature page for each user to acknowledge receipt, indicating that they have read, understand, and agree to abide by the rules of behavior. Electronic signatures are acceptable for use in acknowledging the rules of behavior.

Figure 2 lists examples from OMB Circular A-130 Appendix III of what should be covered in typical rules of behavior. These are examples only and agencies have flexibility in the detail and contents. When developing the rules of behavior, keep in mind that the intent is to make all users accountable for their actions by acknowledging that they have read, understand, and agree to abide by the rules of behavior. The rules should not be a complete copy of the security policy or procedures guide, but rather cover, at a high level, some of the controls described in the following Figure.

[8] In some agencies, the senior official and the Chief Information Officer may be co-authorizing officials. In this situation, the senior official approves the operation of the information system prior to the Chief Information Officer.

Examples of Controls Contained in Rules of Behavior

- Delineate responsibilities, expected use of system, and behavior of all users.
- Describe appropriate limits on interconnections.
- Define service provisions and restoration priorities.
- Describe consequences of behavior not consistent with rules.
- Covers the following topics:
  - Work at home
  - Dial-in access
  - Connection to the Internet
  - Use of copyrighted work
  - Unofficial use of government equipment
  - Assignment and limitations of system privileges and individual accountability
  - Password usage
  - Searching databases and divulging information.

Figure 2: Rules of Behavior Examples

1.9 System Security Plan Approval

Organizational policy should clearly define who is responsible for system security plan approval and procedures developed for plan submission, including any special memorandum language or other documentation required by the agency. Prior to the certification and accreditation process, the designated Authorizing Official, independent from the system owner, typically approves the plan.

2. System Boundary Analysis and Security Controls

Before the system security plan can be developed, the information system and the information resident within that system must be categorized based on a FIPS 199 impact analysis. Then a determination can be made as to which systems in the inventory can be logically grouped into major applications or general support systems. The FIPS 199 impact levels must be considered when the system boundaries are drawn and when selecting the initial set of security controls (i.e., control baseline). The baseline security controls can then be tailored based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, the availability of compensating controls, or special circumstances. Common security controls, which is one of the tailoring considerations, must be identified prior to system security plan preparation in order to identity those controls covered at the agency level, which are not system-specific. These common security controls can then be incorporated into the system security plan by reference.

2.1 System Boundaries

The process of uniquely assigning information resources[9] to an information system defines the security boundary for that system. Agencies have great flexibility in determining what constitutes an information system (i.e., major application or general support system). If a set of information resources is identified as an information system, the resources should generally be under the same direct management control. Direct management control[10] does not necessarily imply that there is no intervening management. It is also possible for an information system to contain multiple *subsystems*.

A subsystem is a major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions. Subsystems typically fall under the same management authority and are included within a single system security plan. Figure 3 depicts a general support system with three subsystems.

In addition to the consideration of direct management control, it may be helpful for agencies to consider if the information resources being identified as an information system:

- Have the same function or mission objective and essentially the same operating characteristics and security needs, and

[9] Information resources consist of information and related resources, such as personnel, equipment, funds, and information technology.

[10] Direct management control typically involves budgetary, programmatic, or operational authority and associated responsibility. For new information systems, management control can be interpreted as having budgetary/programmatic authority and responsibility for the development and deployment of the information systems. For information systems currently in the federal inventory, management control can be interpreted as having budgetary/operational authority for the day-to-day operations and maintenance of the information systems.

- Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).

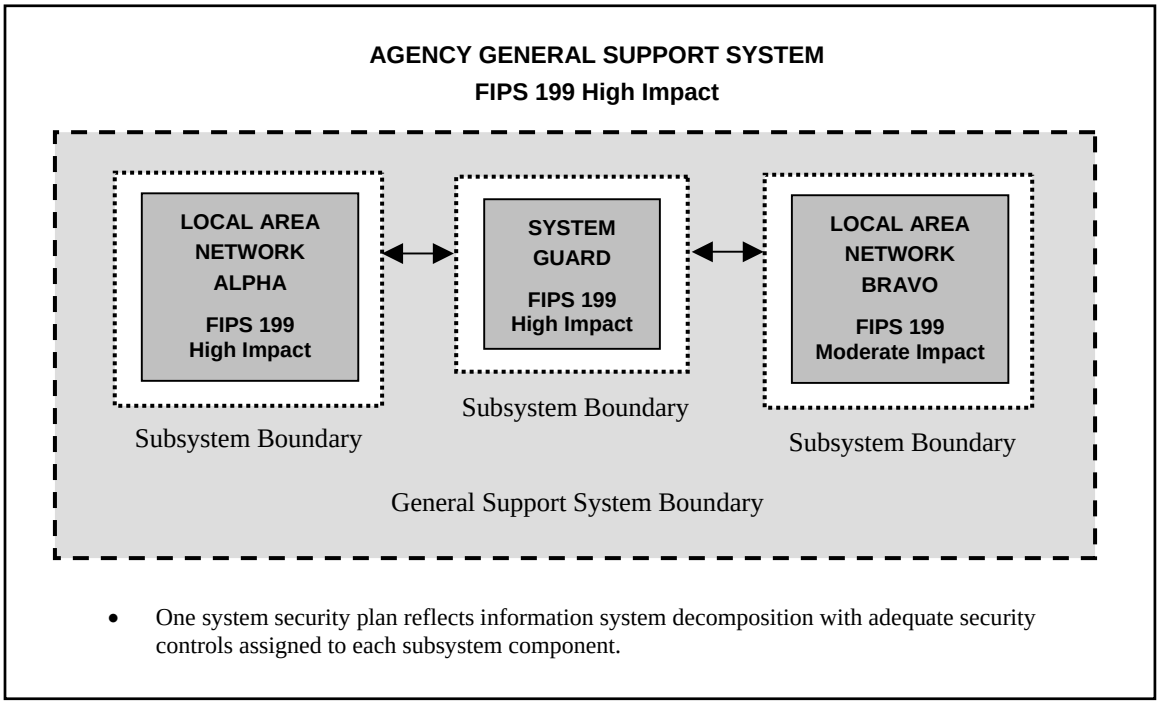


Figure 3: Decomposition of large and complex information systems

While the above considerations may be useful to agencies in determining information system boundaries for purposes of security accreditation, they should not be viewed as limiting the agency's flexibility in establishing boundaries that promote effective information security within the available resources of the agency. Authorizing officials and senior agency information security officers should consult with prospective information system owners when establishing information system boundaries. The process of establishing boundaries for agency information systems and the associated security implications, is an agency-level activity that should include careful negotiation among all key participants—taking into account the mission/business requirements of the agency, the technical considerations with respect to information security, and the programmatic costs to the agency.

FIPS 199 defines security categories for information systems based on potential impact on organizations, assets, or individuals should there be a breach of security—that is, a loss of confidentiality, integrity, or availability. FIPS 199 security categories can play an important part in defining information system boundaries by partitioning the agency's information systems according to the criticality or sensitivity of the information and information systems and the importance of those systems in accomplishing the agency's mission. This is particularly important when there are various FIPS 199 impact levels contained in one information system. The FIPS 199 requirement to secure an information

system to the high watermark or highest impact level must be applied when grouping minor applications/subsystems with varying FIPS 199 impact levels into a single general support system or major application unless there is adequate boundary protection, e.g., firewalls and encryption, around those subsystems or applications with the highest impact level. Additionally, there must be assurance that the shared resources, i.e., networks, communications, and physical access within the whole general support system or major application, are protected adequately for the highest impact level. Having the ability to isolate the high impact systems will not only result in more secure systems, but will also reduce the amount of resources required to secure many applications/systems that do not require that level of security. NIST SP 800-53 provides three security control baselines, i.e., low, moderate, and high, that are associated with the three FIPS 199 impact levels; as the impact level increases, so do the minimum assurance requirements. For reporting purposes, i.e., FISMA annual report, when an information system has varying FIPS 199 impact levels, that system is categorized at the highest impact level on that information system.

2.2 Major Applications

All federal applications have value and require some level of protection. Certain applications, because of the information they contain, process, store, or transmit, or because of their criticality to the agency's mission, require special management oversight. These applications are major applications. A major application is expected to have a FIPS 199 impact level of moderate or high. OMB Circular A-130 defines a "major information system" as an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources. Major applications are by definition major information systems.

Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system). A major application might comprise many individual programs and hardware, software, and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific, mission-related function. A major application may also consist of multiple individual applications if all are related to a single mission function (e.g., payroll or personnel). If a system is defined as a major application and the application is run on another organization's general support system, the major application owner is responsible for acceptance of risk and in addition:

- Notifies the general support system owner that the application is critical and provides specific security requirements;

- Provides a copy of the major application's system security plan to the operator of the general support system;

- Requests a copy of the system security plan of the general support system and ensures that it provides adequate protection for the application and information; and

- Includes a reference to the general support system security plan in the major application system security plan.

2.3 General Support Systems

A general support system is an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example[11], can be a:

- LAN including smart terminals that support a branch office;
- Backbone (e.g., agency-wide);
- Communications network;
- Agency data processing center including its operating system and utilities,
- Tactical radio network; or
- Shared information processing service facility

A general support system can have a FIPS 199 impact level of low, moderate, or high in its security categorization depending on the criticality or sensitivity of the system and any major applications the general support system is supporting. A general support system is considered a major information system when special management attention is required, there are high development, operating, or maintenance costs; and the system/information has a significant role in the administration of agency programs. When the general support system is a major information system, the system's FIPS 199 impact level is either moderate or high.

A major application can be hosted on a general support system. The general support system plan should reference the major application system security plan.

2.4 Minor Applications

Agencies are expected to exercise management judgment in determining which of their applications are minor applications and to ensure that the security requirements of minor applications are addressed as part of the system security plan for the applicable general support systems or, in some cases, the applicable major application. It is very common that a minor application may have a majority of its security controls provided by the general support system or major application on which it resides. If this is the case, the information system owner of the general support system or major application is the information system owner for the minor application and is responsible for developing the

[11] The example provided is a small sampling of general support systems; it is not a definitive list.

system security plan. The additional security controls specific to the minor application should be documented in the system security plan as an appendix or paragraph. The minor application owner (often the same as information owner) may develop the appendix or paragraph describing the additional controls. The complete general support system or major application system security plan should be shared with the information owner.

The minor application can have a FIPS 199 security category of low or moderate. However, if the minor application resides on a system that does not have adequate boundary protection, the minor application must implement the minimum baseline controls required by the host or interconnected system.

2.5 Security Controls

FIPS 200 provides seventeen minimum security requirements for federal information and information systems. The requirements represent a broad-based, balanced information security program that addresses the management, operational, and technical aspects of protecting the confidentiality, integrity, and availability of federal information and information systems. An agency must meet the minimum security requirements in this standard by applying security controls selected in accordance with NIST SP 800-53 and the designated impact levels of the information systems. An agency has the flexibility to tailor the security control baseline in accordance with the terms and conditions set forth in the standard. Tailoring activities include: (i) the application of scoping guidance; (ii) the specification of compensating controls; and (iii) the specification of agency-defined parameters in the security controls, where allowed. The system security plan should document all tailoring activities.

2.5.1 Scoping Guidance

Scoping guidance provides an agency with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines defined in NIST SP 800-53. Several considerations described below can potentially impact how the baseline security controls are applied by the agency. System security plans should clearly identify which security controls employed scoping guidance and include a description of the type of considerations that were made. The application of scoping guidance must be reviewed and approved by the authorizing official for the information system.

Technology-related considerations—

- Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) will only be applicable if those technologies are employed or are required to be employed within the information system.

- Security controls will only be applicable to those components of the information system that typically provide the security capability addressed by the minimum security requirements.

- Security controls that can be either explicitly or implicitly supported by automated mechanisms will not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. In situations where automated mechanisms are not readily available or technically feasible, compensating security controls, implemented through non-automated mechanisms or procedures, will be used to satisfy minimum security requirements.

Common security control-related considerations—

- Security controls designated by the agency as common controls will, in most cases, be managed by an organizational entity other than the information system owner. Every control in a security control baseline must be addressed either by the agency through common security controls or by the information system owner. Decisions on common control designations must not, however, affect the agency's responsibility in providing the necessary security controls required to meet the minimum security requirements for the information system. (Additional information on common controls is provided in Section 2.5.3.)

Public access information systems-related considerations—

- Security controls associated with public access information systems must be carefully considered and applied with discretion since some of the security controls from the specified security control baselines (e.g., personnel security controls, identification and authentication controls) may not be applicable to users accessing information systems through public interfaces.[12]

Infrastructure-related considerations—

- Security controls that refer to agency facilities (e.g., physical access controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) will be applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, controlled interface equipment, and communications equipment).

[12] For example, while the baseline security controls require identification and authentication of organizational personnel who maintain and support information systems that provide public access services, the same controls might not be required for users accessing those systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication must be required for users accessing information systems through public interfaces to access their private/personal information.

Scalability-related considerations—

- Security controls will be scalable by the size and complexity of the particular agency implementing the controls and the impact level of the information system. Scalability addresses the breadth and depth of security control implementation. Discretion is needed in scaling the security controls to the particular environment of use to ensure a cost-effective, risk-based approach to security control implementation.[13]

Risk-related considerations—

- Security controls that uniquely support the confidentiality, integrity, or availability security objectives can be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high watermark;[14] (ii) is supported by an agency's assessment of risk; and (iii) does not affect the security-relevant information within the information system.[15]

2.5.2 Compensating Controls

Compensating security controls are the management, operational, or technical controls employed by an agency in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or comparable protection for an information system. Compensating security controls for an information system will be employed by an agency only under the following conditions: (i) the agency selects the compensating controls from the security control catalog in NIST SP 800-53; (ii) the agency provides a complete and convincing rationale and justification for how the compensating controls provide an equivalent security capability or level of protection for the information system; and (iii) the agency assesses and formally accepts the risk associated with employing the compensating controls in the information system. The use

[13] For example, a contingency plan for a large and complex organization with a moderate-impact or high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for a smaller organization with a low-impact information system may be considerably shorter and contain much less implementation detail.

[14] When employing the "high watermark" concept, some of the security objectives (i.e., confidentiality, integrity, or availability) may have been increased to a higher impact level. As such, the security controls that uniquely support these security objectives will have been upgraded as well. Consequently, organizations must consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[15] Information that is security-relevant at the system level (e.g., password files, network routing tables, cryptographic key management information) must be distinguished from user-level information within an information system. Certain security controls within an information system are used to support the security objectives of confidentiality and integrity for both user-level and system-level information. Organizations must exercise caution in downgrading confidentiality or integrity-related security controls to ensure that the downgrading action does not affect the security-relevant information within the information system.

of compensating security controls must be reviewed, documented in the system security plan, and approved by the authorizing official for the information system.

2.5.3 Common Security Controls

An agency-wide view of the information security program facilitates the identification of common security controls that can be applied to one or more agency information systems. Common security controls can apply to: (i) all agency information systems; (ii) a group of information systems at a specific site (sometimes associated with the terms site certification/accreditation); or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites (sometimes associated with the terms type certification/accreditation). Common security controls, typically identified during a collaborative agency-wide process with the involvement of the CIO, SAISO, authorizing officials, information system owners, and information system security officers (and by developmental program managers in the case of common security controls for common hardware, software, and/or firmware), have the following properties:

- The development, implementation, and assessment of common security controls can be assigned to responsible agency officials or organizational elements (other than the information system owners whose systems will implement or use those common security controls); and

- The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of agency information systems where those controls have been applied.

Many of the management and operational controls (e.g., contingency planning controls, incident response controls, security awareness and training controls, personnel security controls, and physical security controls) needed to protect an information system may be excellent candidates for common security control status. The objective is to reduce security costs by centrally managing the development, implementation, and assessment of the common security controls designated by the agency—and subsequently, sharing assessment results with the owners of information systems where those common security controls are applied. Security controls not designated as common controls are considered *system-specific controls* and are the responsibility of the information system owner. System security plans should clearly identify which security controls have been designated as common security controls and which controls have been designated as system-specific controls.

For efficiency in developing system security plans, common security controls should be documented once and then inserted or imported into each system security plan for the information systems within the agency. The individual responsible for implementing the common control should be listed in the security plan. Effectively maximizing the application of common controls in the system security planning process depends upon the following factors:

- The agency has developed, documented, and communicated its specific guidance on identifying common security controls;

- The agency has assigned the responsibility for coordinating common security control identification and review and obtaining consensus on the common control designations, to a management official with security program responsibilities such as the CIO or SAISO;

- System owners have been briefed on the system security planning process including use of common controls; and

- Agency experts in the common control areas identified have been consulted as part of the process.

An agency may also assign a hybrid status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific. For example, an agency may view the IR-1 (Incident Response Policy and Procedures) security control as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid security controls may also serve as templates for further control refinement. An agency may choose, for example, to implement the CP-2 (Contingency Plan) security control as a master template for a generalized contingency plan for all agency information systems with individual information system owners tailoring the plan, where appropriate, for system-specific issues.

Information system owners are responsible for any system-specific issues associated with the implementation of an agency's common security controls. These issues are identified and described in the system security plans for the individual information systems. The SAISO, acting on behalf of the CIO, should coordinate with agency officials (e.g., facilities managers, site managers, personnel managers) responsible for the development and implementation of the designated common security controls to ensure that the required controls are put into place, the controls are assessed, and the assessment results are shared with the appropriate information system owners.

Partitioning security controls into common security controls and system-specific security controls can result in significant savings to the agency in control development and implementation costs. It can also result in a more consistent application of the security controls across the agency at large. Moreover, equally significant savings can be realized in the security certification and accreditation process. Rather than assessing common security controls in every information system, the certification process draws upon any applicable results from the most current assessment of the common security controls performed at the agency level. An agency-wide approach to reuse and sharing of assessment results can greatly enhance the efficiency of the security certifications and accreditations being conducted by an agency and significantly reduce security program costs.

While the concept of security control partitioning into common security controls and system-specific controls is straightforward and intuitive, the application of this principle within an agency takes planning, coordination, and perseverance. If an agency is just beginning to implement this approach or has only partially implemented this approach, it may take some time to get the maximum benefits from security control partitioning and the associated reuse of assessment evidence. Because of the potential dependence on common security controls by many of an agency's information systems, a failure of such common controls may result in a significant increase in agency-level risk—risk that arises from the operation of the systems that depend on these controls.

3. Plan Development

The remainder of this document guides the reader in writing a system security plan, including logical steps which should be followed in approaching plan development, recommended structure and content, and how to maximize the use of current NIST publications to effectively support system security planning activity. There should be established agency policy on how the information system security plans are to be controlled and accessed prior to initiation of the activity.

3.1 System Name and Identifier

The first item listed in the system security plan is the system name and identifier. As required in OMB Circular A-11, each system should be assigned a name and unique identifier. Assignment of a unique identifier supports the agency's ability to easily collect agency information and security metrics specific to the system as well as facilitate complete traceability to all requirements related to system implementation and performance. This identifier should remain the same throughout the life of the system and be retained in audit logs related to system use.

3.2 System Categorization

Each system identified in the agency's system inventory must be categorized using FIPS 199. NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides implementation guidance in completing this activity. See Table 1 for a summary of FIPS 199 categories.

3.3 System Owner

A designated system owner must be identified in the system security plan for each system. This person is the key point of contact (POC) for the system and is responsible for coordinating system development life cycle (SDLC) activities specific to the system. It is important that this person have expert knowledge of the system capabilities and functionality. The assignment of a system owner should be documented in writing and the plan should include the following contact information:

- Name
- Title
- Agency
- Address
- Phone Number
- Email Address

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 1: FIPS 199 Categorization

3.4 Authorizing Official

An authorizing official must be identified in the system security plan for each system. This person is the senior management official who has the authority to authorize operation (accredit) of an information system (major application or general support system) and accept the residual risk associated with the system. The assignment of the authorizing official should be in writing, and the plan must include the same contact information listed in Section 3.3.

3.5 Other Designated Contacts

This section should include names of other key contact personnel who can address inquiries regarding system characteristics and operation. The same information listed in Section 3.3 should be included for each person listed under this section.

3.6 Assignment of Security Responsibility

Within an agency, an individual must be assigned responsibility for each system. This can be accomplished in many ways. In some agencies, the overall responsibility may be delegated to the SAISO. Often, the SAISO is supported by a subnet of security officers assigned to each major component. These security officers may be authorized to address the security requirements for all systems within their domain of authority. Other models may segment this responsibility in other ways based on agency structure and responsibility. The same contact information, as listed under Section 3.3, should be provided for these individuals. Most important is that this responsibility be formalized in writing either in the employee's Position Description or by delegation Memorandum.

3.7 System Operational Status

Indicate one or more of the following for the system's operational status. If more than one status is selected, list which part of the system is covered under each status.

- *Operational* — the system is in production.
- *Under Development* — the system is being designed, developed, or implemented.
- *Undergoing a major modification* — the system is undergoing a major conversion or transition.

If the system is under development or undergoing a major modification, provide information about the methods used to assure that up-front security requirements are included. Include specific controls in the appropriate sections of the plan depending on where the system is in the security life cycle.

3.8 Information System Type

In this section of the plan, indicate whether the system is a major application or general support system. If the system contains minor applications, describe them in the General Description/Purpose section of the plan. If the agency has additional categories of information system types, modify the template to include the other categories.

3.9 General Description/Purpose

Prepare a brief description (one to three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an agency, business census data analysis, crop reporting support).

If the system is a general support system, list all applications supported by the general support system. Specify if the application is or is not a major application and include unique name/identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations, whether they are internal or external to the system owner's agency.

3.10 System Environment

Provide a brief (one to three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as use of Personal Digital Assistants, wireless technology, etc. Typically, operational environments are as follows:

- **Standalone or Small Office/Home Office (SOHO)** describes small, informal computer installations that are used for home or business purposes. Standalone encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems, to small businesses and small branch offices of a company.

- **Managed or Enterprise** are typically large agency systems with defined, organized suites of hardware and software configurations, usually consisting of centrally managed workstations and servers protected from the Internet by firewalls and other network security devices.

- **Custom** environments contain systems in which the functionality and degree of security do not fit the other environments. Two typical Custom environments are **Specialized Security-Limited Functionality and Legacy**:

  -- **Specialized Security-Limited Functionality**. A Specialized Security-Limited Functionality environment contains systems and networks at high risk of attack or data exposure, with security taking precedence over functionality. It assumes systems have limited or specialized (not general purpose workstations or systems) functionality in a highly threatened environment such as an outward facing firewall or public web server or whose data content or mission purpose is of such value that aggressive trade-offs in favor of security outweigh the potential negative consequences to other useful system attributes such as legacy applications or interoperability with other systems. A Specialized Security-Limited Functionality environment could be a subset of another environment.

  -- **Legacy**. A Legacy environment contains older systems or applications that may use older, less-secure communication mechanisms. Other machines operating in a Legacy environment may need less restrictive security settings so that they can communicate with legacy systems and applications. A Legacy environment could be a subset of a standalone or managed environment.[16]

[16] For a detailed explanation of system environments, see NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products -- Guidance for Checklists Users and Developers.*

3.11 System Interconnection/Information Sharing

System interconnection is the direct connection of two or more IT systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system owners, information owners, and management obtain as much information as possible regarding vulnerabilities associated with system interconnections and information sharing. This is essential to selecting the appropriate controls required to mitigate those vulnerabilities. An Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or Memorandum of Agreement (MOA) is needed between systems (not between workstations/desktops or publicly accessed systems) that share data that are owned or operated by different organizations. An ISA is not needed with internal agency systems if an agency manages and enforces a rigid system development life cycle, which requires approvals and sign-offs ensuring compliance with security requirements. For additional information on interconnections, see NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems.*

In this section, for ***each interconnection*** between systems that are owned or operated by different organizations, provide the following information concerning the authorization for the connection to other systems or the sharing of information:

- Name of system;
- Organization;
- Type of interconnection (Internet, Dial-Up, etc.);
- Authorizations for interconnection (MOU/MOA, ISA);
- Date of agreement;
- FIPS 199 Category;
- Certification and accreditation status of system; and
- Name and title of authorizing official(s).

For agencies with numerous interconnections, a table format including the above information may be a good way to present the information.

3.12 Laws, Regulations, and Policies Affecting the System

List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of the system and information retained by, transmitted by, or processed by the system. General agency security requirements need

not be listed since they mandate security for all systems. Each agency should decide on the level of laws, regulations, and policies to include in the system security plan. Examples might include the Privacy Act of 1974 or a specific statute or regulation concerning the information processed (e.g., tax or census information). If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.

3.13 Security Control Selection

In preparation for documenting how the NIST SP 800-53 security controls for the applicable security control baseline (low-, moderate-, or high impact information systems) are implemented or planned to be implemented, the security controls contained in the baseline should be reviewed and possibly tailored. The scoping guidelines explained in Section 2.5.1 should be used when determining the applicability or tailoring of individual controls. Additionally the controls that are common among numerous systems or within the whole agency should be identified and then documented in the plan. See Section 2.5.3 for guidance on how the common controls should be determined, documented, and coordinated. The process of selecting the appropriate security controls and applying the scoping guidelines to achieve *adequate security*[17] is a multifaceted, risk-based activity involving management and operational personnel within the agency and should be conducted before the security control portion of the plan is written.

- For *low-impact* information systems, an agency must, as a minimum, employ the security controls from the low baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the low baseline are satisfied.

- For *moderate-impact* information systems, an agency must, as a minimum, employ the security controls from the moderate baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the moderate baseline are satisfied.

- For *high-impact* information systems, an agency must, as a minimum, employ the security controls from the high baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements associated with the high baseline are satisfied.

3.14 Minimum Security Controls

Now that the security controls have been selected, tailored, and the common controls identified, describe each control. The description should contain 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3)

[17] The Office of Management and Budget (OMB) Circular A-130, Appendix III, defines adequate security as security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.

Security controls in the security control catalog (NIST SP 800-53, Appendix F) have a well-defined organization and structure. The security controls are organized into classes and families for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical[18]). Each family contains security controls related to the security function of the family. A standardized, two-character identifier is assigned to uniquely identify each control family. Table 2 summarizes the classes and families in the security control catalog and the associated family identifiers.

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

Security control class designations (i.e., management, operational, and technical) are defined below for clarification in preparation of system security plans.
Management controls focus on the management of the information system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. ***Operational controls*** address security methods focusing on

[18] Security control families in NIST SP 800-53 are associated with one of three security control classes (i.e., management, operational, technical). Families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning family, is listed as an operational control but also has characteristics that are consistent with security management as well.

mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. ***Technical controls*** focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

3.15 Completion and Approval Dates

The completion date of the system security plan should be provided. The completion date should be updated whenever the plan is periodically reviewed and updated. When the system is updated, a version number should be added. The system security plan should also contain the date the authorizing official or the designated approving authority approved the plan. Approval documentation, i.e., accreditation letter, approval memorandum, should be on file or attached as part of the plan.

3.16 Ongoing System Security Plan Maintenance

Once the information system security plan is developed, it is important to periodically assess the plan, review any change in system status, functionality, design, etc., and ensure that the plan continues to reflect the correct information about the system. This documentation and its correctness are critical for system certification activity. All plans should be reviewed and updated, if appropriate, at least annually. Some items to include in the review are:

- Change in information system owner;
- Change in information security representative;
- Change in system architecture;
- Change in system status;
- Additions/deletions of system interconnections;
- Change in system scope;
- Change in authorizing official; and
- Change in certification and accreditation status.

Appendix A: Sample Information System Security Plan Template

The following sample has been provided ONLY as one example. Agencies may be using other formats and choose to update those to reflect any existing omissions based on this guidance. This is not a mandatory format; it is recognized that numerous agencies and information security service providers may have developed and implemented various approaches for information system security plan development and presentation to suit their own needs for flexibility.

Information System Security Plan Template

1. Information System Name/Title:

- Unique identifier and name given to the system.

2. Information System Categorization:

- Identify the appropriate FIPS 199 categorization.

	LOW		**MODERATE**		**HIGH**

3. Information System Owner:

- Name, title, agency, address, email address, and phone number of person who owns the system.

4. Authorizing Official:

- Name, title, agency, address, email address, and phone number of the senior management official designated as the authorizing official.

5. Other Designated Contacts:

- List other key personnel, if applicable; include their title, address, email address, and phone number.

6. Assignment of Security Responsibility:

- Name, title, address, email address, and phone number of person who is responsible for the security of the system.

7. Information System Operational Status:

- Indicate the operational status of the system. If more than one status is selected, list which part of the system is covered under each status.

	Operational		**Under Development**		**Major Modification**

8. Information System Type:

- Indicate if the system is a major application or a general support system. If the system contains minor applications, list them in Section 9. General System Description/Purpose.

	Major Application		**General Support System**

9. General System Description/Purpose

- Describe the function or purpose of the system and the information processes.

10. System Environment

- Provide a general description of the technical system. Include the primary hardware, software, and communications equipment.

11. System Interconnections/Information Sharing

- List interconnected systems and system identifiers (if appropriate), provide the system, name, organization, system type (major application or general support system), indicate if there is an ISA/MOU/MOA on file, date of agreement to interconnect, FIPS 199 category, C&A status, and the name of the authorizing official.

System Name	Organization	Type	Agreement (ISA/MOU/MOA)	Date	FIPS 199 Category	C&A Status	Auth. Official

12. Related Laws/Regulations/Policies

- List any laws or regulations that establish specific requirements for the confidentiality, integrity, or availability of the data in the system.

13. Minimum Security Controls

Select the appropriate minimum security control baseline (low-, moderate-, high-impact) from NIST SP 800-53, then provide a thorough description of how all the minimum security controls in the applicable baseline are being implemented or planned to be implemented. The description should contain: 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation.

14. Information System Security Plan Completion Date: _____

- Enter the completion date of the plan.

15. Information System Security Plan Approval Date: _____

- Enter the date the system security plan was approved and indicate if the approval documentation is attached or on file.

Appendix B: Glossary

COMMON TERMS AND DEFINITIONS

Accreditation [NIST SP 800-37]	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary [NIST SP 800-37]	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.
Accrediting Authority	See Authorizing Official.
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorize Processing	See Accreditation.
Authorizing Official [NIST SP 800-37]	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.

Certification [NIST SP 800-37]	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification Agent [NIST SP 800-37]	The individual, group, or organization responsible for conducting a security certification.
Chief Information Officer [44 U.S.C., Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, executive orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.
Common Security Control [NIST SP 800-37]	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, that provide equivalent or comparable protection for an information system.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to ensure that the information system is protected against improper modifications before, during, and after system implementation.
Countermeasures [CNSS Inst. 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
General Support System [OMB Circular A-130, Appendix III]	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
High-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Information Owner [CNSS Inst. 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, executive order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Label	See Security Label.
Low-Impact System	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Major Application [OMB Circular A-130, Appendix III]	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
Major Information System [OMB Circular A-130]	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Management Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Media Access Control Address	A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.
Minor Application	An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Moderate-Impact System	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.
National Security Emergency Preparedness Telecommunications Services	Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Non-repudiation [CNSS Inst. 4009]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).

Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privacy Impact Assessment [OMB Memorandum 03-22]	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Records	The recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Remote Access	Access by users (or information systems) communicating external to an information system security perimeter.
Remote Maintenance	Maintenance activities conducted by individuals communicating external to an information system security perimeter.
Risk [NIST SP 800-30]	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment [NIST SP 800-30]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management, synonymous with risk analysis, and incorporates threat and vulnerability analyses.
Risk Management [NIST SP 800-30]	The process of managing risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system. It includes risk assessment; cost-benefit analysis; the selection, implementation, and assessment of security controls; and the formal authorization to operate the system. The process considers effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.
Safeguards [CNSS Inst. 4009, Adapted]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization [CNSS Inst. 4009, Adapted]	Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.
Scoping Guidance	Provides organizations with specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security controls in the control baseline.
Security Category [FIPS 199]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Baseline	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

Security Impact Analysis [NIST SP 800-37]	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security Objective	Confidentiality, integrity, or availability.
Security Perimeter	See Accreditation Boundary.
Security Plan	See System Security Plan.
Security Requirements	Requirements levied on an information system that are derived from laws, executive orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one or more specific functions.
System	See Information System.
System-specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common security control.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Technical Controls [NIST SP 800-18]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat [CNSS Inst. 4009, Adapted]	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Agent/Source [NIST SP 800-30]	Either: (i) intent and method targeted at the intentional exploitation of a vulnerability; or (ii) a situation and method that may accidentally trigger a vulnerability.
Threat Assessment [CNSS Inst. 4009]	Formal description and evaluation of threat to an information system.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
User [CNSS Inst. 4009]	Individual or (system) process authorized to access an information system.
Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSS Inst. 4009]	Formal description and evaluation of the vulnerabilities in an information system.

Appendix C: References

Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.

Federal Information Processing Standards Publication 200, *Security Controls for Federal Information System*, (projected for publication February 2006).

Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.

National Institute of Standards and Technology Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, November 2001.

National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, February 2005.

National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle*, June 2004.

National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products -- Guidance for Checklists Users and Developers*, May 2005.

Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

NIST Special Publication 800-26

Security Self-Assessment Guide for Information Technology Systems

Marianne Swanson

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

C O M P U T E R S E C U R I T Y

NIST CENTENNIAL 1901-2001

NIST Special Publication 800-26

Security Self-Assessment Guide for Information Technology Systems

Marianne Swanson

C O M P U T E R S E C U R I T Y

November 2001

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Karen H. Brown, Acting Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Karen H. Brown, Acting Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Acknowledgements

Many people have contributed to this document, directly or indirectly. I would like to thank our NIST Technical Editor, Elizabeth Lennon, for spending a significant amount of her time editing this document. The questionnaire was field tested by Jim Craft, U.S. Agency for International Development, who provided a team to use the questionnaire on two systems. His team's input was invaluable in finalizing the document. I would also like to thank the many people who have provided comments on the draft and expressed their enthusiasm and support for the document. The development of the document was a consolidated effort by many people.

Executive Summary

Adequate security of information and the systems that process it is a fundamental management responsibility. Agency officials must understand the current status of their information security program and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security.

This document builds on the *Federal IT Security Assessment Framework* (Framework) developed by NIST for the Federal Chief Information Officer (CIO) Council. The Framework established the groundwork for standardizing on five levels of security status and criteria agencies could use to determine if the five levels were adequately implemented. This document provides guidance on applying the Framework by identifying 17 control areas, such as those pertaining to identification and authentication and contingency planning. In addition, the guide provides control objectives and techniques that can be measured for each area.

The questionnaire can be used for the following purposes:

- Agency managers who know their agency's systems and security controls can quickly gain a general understanding of needed security improvements for a system (major application or general support system), group of interconnected systems, or the entire agency.

- The security of an agency's system can be thoroughly evaluated using the questionnaire as a guide. The results of such a thorough review produce a reliable measure of security effectiveness and may be used to 1) fulfill reporting requirements; 2) prepare for audits; and 3) identify resources.

- The results of the questionnaire will assist, but not fulfill, agency budget requests as outlined in Office of Management and Budget (OMB) Circular A-11, "Preparing and Submitting Budget Estimates."

It is important to note that the questionnaire is not intended to be an all-inclusive list of control objectives and related techniques. Accordingly, it should be used in conjunction with the more detailed guidance listed in Appendix B. In addition, details associated with certain technical controls are not specifically provided due to their voluminous and dynamic nature. Agency managers should obtain information on such controls from other sources, such as vendors, and use that information to supplement this guide.

Consistent with OMB policy, each agency must implement and maintain a program to adequately secure its information and system assets. An agency program must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification. Performing a self-assessment and mitigating any of the weaknesses found in the assessment is one way to determine if the system and the information are adequately secured.

Table of Contents

1. Introduction

A self-assessment conducted on a system (major application or general support system) or multiple self-assessments conducted for a group of interconnected systems (internal or external to the agency) is one method used to measure information technology (IT) security assurance. IT security assurance is the degree of confidence one has that the managerial, technical and operational security measures work as intended to protect the system and the information it processes. Adequate security of these assets is a fundamental management responsibility. Consistent with Office of Management and Budget (OMB) policy, each agency must implement and maintain a program to adequately secure its information and system assets. Agency programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

Agencies must plan for security, ensure that the appropriate officials are assigned security responsibility, and authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

An important element of ensuring an organizations' IT security health is performing routine self-assessments of the agency security program. For a self-assessment to be effective, a risk assessment should be conducted in conjunction with or prior to the self-assessment. A self-assessment does not eliminate the need for a risk assessment.

There are many methods and tools for agency officials to help determine the current status of their security programs relative to existing policy. Ideally many of these methods and tools would be implemented on an ongoing basis to systematically identify programmatic weaknesses and where necessary, establish targets for continuing improvement. This document provides a method to evaluate the security of unclassified systems or groups of systems; it guides the reader in performing an IT security self-assessment. Additionally, the document provides guidance on utilizing the results of the system self-assessment to ascertain the status of the agency-wide security program. The results are obtained in a form that can readily be used to determine which of the five levels specified in the Federal IT Security Assessment Framework the agency has achieved for each topic area covered in the questionnaire. For example, the group of systems under review may have reached level 4 (Tested and Evaluated Procedures and Controls) in the topic area of physical and environmental protection, but only level 3 (Implemented Procedures and Controls) in the area of logical access controls.

1.1 Self -Assessments

This self-assessment guide utilizes an extensive questionnaire (Appendix A) containing specific control objectives and suggested techniques against which the security of a system or

group of interconnected systems can be measured. The questionnaire can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls. This guide does not establish new security requirements. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. However the guide is not intended to be a comprehensive list of control objectives and related techniques. The guide should be used in conjunction with the more detailed guidance listed in Appendix B. In addition, specific technical controls, such as those related to individual technologies or vendors, are not specifically provided due to their volume and dynamic nature. It should also be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. Each agency should decide if additional security controls should be added to the questionnaire and, if so, customize the questionnaire appropriately.

The goal of this document is to provide a standardized approach to assessing a system. This document strives to blend the control objectives found in the many requirement and guidance documents. To assist the reader, a reference source is listed after each control objective question listed in the questionnaire. Specific attention was made to the control activities found in the General Accounting Office's (GAO) Federal Information System Control Audit Manual (FISCAM). FISCAM is the document GAO auditors and agency inspector generals use when auditing an agency. When FISCAM is referenced in the questionnaire, the major category initials along with the control activity number are provided, e.g., *FISCAM SP-3.1*. The cross mapping of the two documents will form a road map between the control objectives and techniques the audit community assess and the control objectives and techniques IT security program managers and program officials need to assess. The mapping provides a common point of reference for individuals fulfilling differing roles in the assessment process. The mapping ensures that both parties are reviewing the same types of controls.

The questionnaire may be used to assess the status of security controls for a system, an interconnected group of systems, or agency-wide. These systems include information, individual systems (e.g., major applications, general support systems, mission critical systems), or a logically related grouping of systems that support operational programs (e.g., Air Traffic Control, Medicare, Student Aid). Assessing all security controls and all interconnected system dependencies provides a metric of the IT security conditions of an agency. By using the procedures outlined in Chapter 4, the results of the assessment can be used as input on the status of an agency's IT security program.

1.2 Federal IT Security Assessment Framework

The Federal IT Security Assessment Framework issued by the federal Chief Information Officer Council in November 2000 provides a tool that agencies can use to routinely evaluate the status of their IT security programs. The document established the groundwork for standardizing on five levels of security effectiveness and measurements that agencies could use to determine which of the five levels are met. By utilizing the Framework levels, an agency can prioritize agency efforts as well as use the document over time to evaluate progress. The NIST Self-Assessment Guide builds on the Framework by providing questions on specific areas of control, such as those pertaining to access and service continuity, and a means of categorizing evaluation results in the same manner as the Framework. See Appendix C for a copy of the Framework.

1.3 Audience

The control objectives and techniques presented are generic and can be applied to organizations in private and public sectors. This document can be used by all levels of management and by those individuals responsible for IT security at the system level and organization level. Additionally, internal and external auditors may use the questionnaire to guide their review of the IT security of systems. To perform the examination and testing required to complete the questionnaire, the assessor must be familiar with and able to apply a core knowledge set of IT security basics needed to protect information and systems. In some cases, especially in the area of examining and testing technical controls, assessors with specialized technical expertise will be needed to ensure that the questionnaire's answers are reliable.

1.4 Structure of this Document

Chapter 1 introduces the document and explains IT security assessments and the relationship to other documents. Chapter 2 provides a method for determining the system boundaries and criticality of the data. Chapter 3 describes the questionnaire. Chapter 4 provides guidance on using the completed system questionnaire(s) as input into obtaining an assessment of an agency-wide IT security program. Appendix A contains the questionnaire. Appendix B lists the documents used in compiling the assessment control objective questions. Appendix C contains a copy of the *Federal IT Security Assessment Framework*. Appendix D lists references used in developing this document.

2. System Analysis

The questionnaire is a tool for completing an internal assessment of the controls in place for a major application or a general support system. The security of every system or group of interconnected system(s) must be described in a security plan. The system may consist of a major application or be part of a general support system. The definition of major application and general support system are contained in Appendix C. Before the questionnaire can be used effectively, a determination must be made as to the boundaries of the system and the sensitivity and criticality of the information stored within, processed by, or transmitted by the system(s). A completed general support system or major application security plan, which is required under OMB Circular A-130, Appendix III, should describe the boundaries of the system and the criticality level of the data. If a plan has not been prepared for the system, the completion of this self-assessment will aid in developing the system security plan. Many of the control objectives addressed in the assessment are to be described in the system security plan. The following two sections, Section 2.1 and Section 2.2, contain excerpts from NIST Special Publication 800-18*, Guide for Developing Security Plans for Information Technology Systems,* and will assist the reader in determining the physical and logical boundaries of the system and the criticality of the information.

2.1 System Boundaries

Defining the scope of the assessment requires an analysis of system boundaries and organizational responsibilities. Networked systems make the boundaries much harder to define. Many organizations have distributed client-server architectures where servers and workstations communicate through networks. Those same networks are connected to the Internet. A system, as defined in NIST Special Publication 800-18*, Guide for Developing Security Plans for Information Technology Systems*, is identified by defining boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a system security plan and a security evaluation whenever a major modification to the system occurs. Each element of the system must[1]:

- Be under the **same** direct management control;
- Have the **same** function or mission objective;
- Have essentially the **same** operating characteristics and security needs; and
- Reside in the **same** general operating environment.

All components of a system need not be physically connected (e.g., [1] a group of stand-alone personal computers (PCs) in an office; [2] a group of PCs placed in employees' homes under defined telecommuting program rules; [3] a group of portable PCs provided to employees who require mobile computing capability to perform their jobs; and [4] a system

[1] OMB Circular A-130, Appendix III defines general support system or "system" in similar terms.

with multiple identical configurations that are installed in locations with the same environmental and physical controls).

An important element of the assessment will be determining the effectiveness of the boundary controls when the system is part of a network. The boundary controls must protect the defined system or group of systems from unauthorized intrusions. If such boundary controls are not effective, then the security of the systems under review will depend on the security of the other systems connected to it. In the absence of effective boundary controls, the assessor should determine and document the adequacy of controls related to each system that is connected to the system under review.

2.2 Sensitivity Assessment

Effective use of the questionnaire presumes a comprehensive understanding of the value of the systems and information being assessed. Value can be expressed in terms of the degree of sensitivity or criticality of the systems and information relative to each of the five protection categories in section 3534(a)(1)(A) of the Government Information Security Reform provisions of the National Defense Authorization Act of 2000, i.e., integrity, confidentiality, availability, authenticity, and non-repudiation. The addition of authenticity and non-repudiation as protection categories within the Reform Act was to stress the need for these assurances as the government progresses towards a paperless workplace. There are differing opinions on what constitutes protection categories, for continuity within several NIST Special Publication 800 documents; authenticity, non-repudiation, and accountability are associated with the integrity of the information.

- ***Confidentiality*** - The information requires protection from unauthorized disclosure.
- ***Integrity*** - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:
    - *Authenticity* – A third party must be able to verify that the content of a message has not been changed in transit.
    - *Non-repudiation* – The origin or the receipt of a specific message must be verifiable by a third party.
    - *Accountability* - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- ***Availability*** - The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.

When determining the value, consider any laws, regulations, or policies that establish specific requirements for integrity, confidentiality, authenticity, availability, and non-repudiation of data and information in the system. Examples might include Presidential Decision Directive 63, the Privacy Act, or a specific statute or regulation concerning the information processed (e.g., tax or census information).

Consider the information processed by the system and the need for protective measures. Relate the information processed to each of the three basic protection requirements above (**confidentiality**, **integrity**, and **availability).** In addition, it is helpful to categorize the system or group of systems by sensitivity level. Three examples of such categories for sensitive unclassified information are described below:

- *High* — Extremely grave injury accrues to U.S. interests if the information is compromised; could cause loss of life, imprisonment, major financial loss, or require legal action for correction

- *Medium*—Serious injury accrues to U.S. interests if the information is compromised; could cause significant financial loss or require legal action for correction

- *Low* —Injury accrues to U.S. interests if the information is compromised; would cause only minor financial loss or require only administrative action for correction

For example, a system and its information may require a high degree of integrity and availability, yet have no need for confidentiality.

Many agencies have developed their own methods of making these determinations. Regardless of the method used, the system owner/program official is responsible for determining the sensitivity of the system and information. The sensitivity should be considered as each control objective question in the questionnaire is answered. When a determination is made to either provide more rigid controls than are addressed by the questionnaire or not to implement the control either temporarily or permanently, there is a risk based decision field in the questionnaire that can be checked to indicate that a determination was made. The determination for lesser or more stringent protection should be made due to either the sensitivity of the data and operations affected or because there are compensating controls that lessen the need for this particular control technique. It should be noted in the comments section of the questionnaire that the system security plan contains supporting documentation as to why the specific control has or has not been implemented.

3. Questionnaire Structure

The self-assessment questionnaire contains three sections: cover sheet, questions, and notes. The questionnaire begins with a cover sheet requiring descriptive information about the major application, general support system, or group of interconnected systems being assessed. The questionnaire provides a hierarchical approach to assessing a system by containing critical elements and subordinate questions. The critical element level should be determined based on the answers to the subordinate questions. The critical elements are derived primarily from OMB Circular A-130. The subordinate questions address the control objectives and techniques that can be implemented to meet the critical elements. Assessors will need to carefully review the levels of subordinate control objectives and techniques in order to determine what level has been reached for the related critical element. The control objectives were obtained from the list of source documents located in Appendix B. There is flexibility in implementing the control objectives and techniques. It is feasible that not all control objectives and techniques may be needed to achieve the critical element.

The questionnaire section may be customized by the organization. An organization can add questions, require more descriptive information, and even pre-mark certain questions if applicable. For example, many agencies may have personnel security procedures that apply to all systems within the agency. The level 1 and level 2 columns in the questionnaire can be pre-marked to reflect the standard personnel procedures in place. Additional columns may be added to reflect the status of the control, i.e., planned action date, non-applicable, or location of documentation. The questionnaire should not have questions removed or questions modified to reduce the effectiveness of the control.

After each question, there is a comment field and an initial field. The comment field can be used to note the reference to supporting documentation that is attached to the questionnaire or is obtainable for that question. The initial field can be used when a risk based decision is made concerning not to implement a control or if the control is not applicable for the system. At the end of each set of questions, there is an area provided for notes. This area may be used for denoting where in a system security plan specific sections should be modified. It can be used to document the justification as to why a control objective is not being implemented fully or why it is overly rigorous. The note section may be a good place to mark where follow-up is needed or additional testing, such as penetration testing or product evaluations, needs to be initiated. Additionally, the section may reference supporting documentation on how the control objectives and techniques were tested and a summary of findings.

3.1 Questionnaire Cover Sheet

This section provides instruction on completing the questionnaire cover sheet, standardizing on how the completed evaluation should be marked, how systems are titled, and labeling the criticality of the system.

3.1.1 Questionnaire Control

All completed questionnaires should be marked, handled, and controlled at the level of sensitivity determined by organizational policy. It should be noted that the information

contained in a completed questionnaire could easily depict where the system or group of systems is most vulnerable.

3.1.2 System Identification

The cover page of the questionnaire begins with the name and title of the system to be evaluated. As explained in NIST Special Publication 800-18, each major application or general support system should be assigned a unique name/identifier.

Assigning a unique identifier to each system helps to ensure that appropriate security requirements are met based on the unique requirements for the system, and that allocated resources are appropriately applied. Further, the use of unique system identifiers is integral to the IT system investment models and analyses established under the requirements of the Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act). The identifiers are required by OMB Circular A-11 and used in the annual OMB budget submissions of the Exhibit 53 and 300. In light of OMB policies concerning capital planning and investment control, the unique name/identifier should remain the same throughout the life of the system to allow the organization to track completion of security requirements over time. Please see OMB Circular A-11, Section 53.7 for additional information on assigning unique identifiers. If no unique name/identifier has been assigned or is not known, contact the information resource management office for assistance.

In many cases the major application or general support system will contain interconnected systems. The connected systems should be listed and once the assessment is complete, a determination should be made and noted on the cover sheet as to whether the boundary controls are effective. The boundary controls should be part of the assessment. If the boundary controls are not adequate, the connected systems should be assessed as well.

The line below the System Name and Title requires the assessor to mark the system category (General Support or Major Application). If an agency has additional system types or system categories, i.e., mission critical or non-mission critical, the cover sheet should be customized to include them.

3.1.3 Purpose and Assessor Information

The purpose and objectives of the assessment should be identified. For example, the assessment is intended to gain a high-level indication of system security in preparation for a more detailed review or the assessment is intended to be a thorough and reliable evaluation for purposes of developing an action plan. The name, title, and organization of the individuals who perform the assessment should be listed. The organization should customize the cover page accordingly.

The start date and completion date of the evaluation should be listed. The length of time required to complete an evaluation will vary. The time and resources needed to complete the assessment will vary depending on the size and complexity of the system, accessibility of system and user data, and how much information is readily available for the assessors to evaluate. For example, if a system has undergone extensive testing, certification, and

documentation, the self-assessment is easy to use and serves as a baseline for future evaluations. If the system has undergone very limited amounts of testing and has poor documentation, completing the questionnaire will require more time.

3.1.4 Criticality of Information

The level of sensitivity of information as determined by the program official or system owner should be documented using the table on the questionnaire cover sheet. If an organization has designed their own method of determining system criticality or sensitivity, the table should be replaced with the organization's criticality or sensitivity categories. The premise behind formulating the level of sensitivity is that systems supporting higher risk operations would be expected to have more stringent controls than those that support lower risk operations.

3.2 Questions

The questions are separated into three major control areas: 1) management controls, 2) operational controls, and 3) technical controls. The division of control areas in this manner complements three other NIST Special Publications: NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook* (Handbook), NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (Principles and Practices), and NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems* (Planning Guide). All three documents should be referenced for further information. The Handbook should be used to obtain additional detail for any of the questions (control objectives) listed in the questionnaire. The Principles and Practices document should be used as a reference to describe the security controls. The Planning Guide formed the basis for the questions listed in the questionnaire. The documents can be obtained from the NIST Computer Security Resource Center web site at the URL: http://csrc.nist.gov.

The questions portion of this document easily maps to the three NIST documents described above since the chapters in all three documents are organized by the same control areas, i.e., management, operational, and technical.

Within each of the three control areas, there are a number of topics; for example, personnel security, contingency planning, and incident response are topics found under the operational control area. There are a total of 17 topics contained in the questionnaire; each topic contains critical elements and supporting security control objectives and techniques (questions) about the system. The critical elements are derived primarily from OMB Circular A-130 and are integral to an effective IT security program. The control objectives and techniques support the critical elements. If a number of the control objectives and techniques are not implemented, the critical elements have not been met.

Each control objective and technique may or may not be implemented depending on the system and the risk associated with the system. Under each control objective and technique question, one or more of the source documents is referenced. The reference points to the

specific control activity in the GAO FISCAM document or to the title of any of the other documents listed in Appendix B, Source of Control Criteria.

Management Controls
1. Risk Management
2. Review of Security Controls
3. Life Cycle
4. Authorize Processing (Certification and Accreditation)
5. System Security Plan

Operational Controls
6. Personnel Security
7. Physical Security
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and Systems Software Maintenance
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

Technical Controls
15. Identification and Authentication
16. Logical Access Controls
17. Audit Trails

Figure 1. Topic Areas

In order to measure the progress of effectively implementing the needed security control, five levels of effectiveness are provided for each answer to the security control question:

- Level 1 – control objective documented in a security policy
- Level 2 – security controls documented as procedures
- Level 3 – procedures have been implemented
- Level 4 – procedures and security controls are tested and reviewed
- Level 5 – procedures and security controls are fully integrated into a comprehensive program.

The method for answering the questions can be based primarily on an examination of relevant documentation and a rigorous examination and test of the controls. The review, for example, should consist of testing the access control methods in place by performing a penetration test; examining system documentation such as software change requests forms, test plans, and approvals; and examining security logs and audit trails. Supporting documentation describing what has been tested and the results of the tests add value to the assessment and will make the next review of the system easier.

Once the checklist, including all references, is completed for the first time, future assessments of the system will require considerably less effort. The completed questionnaire would establish a baseline. If this year's assessment indicates that most of the controls in place are at level 2 or level 3, then that would be the starting point for the next evaluation. More time can be spent identifying ways to increase the level of effectiveness instead of having to gather all the initial information again. Use the comment section to list whether there is supporting documentation and the notes section for any lengthy explanations.

The audit techniques to test the implementation or effectiveness of each control objective and technique are beyond the scope of this document. The GAO FISCAM document provides audit techniques that can be used to test the control objectives.

When answering the questions about whether a specific control objective has been met, consider the sensitivity of the system. The questionnaire contains a field that can be checked when a risk-based decision has been made to either reduce or enhance a security control. There may be certain situations where management will grant a waiver either because compensating controls exists or because the benefits of operating without the control (at least temporarily) outweigh the risk of waiting for full control implementation. Alternatively, there may be times when management implements more stringent controls than generally applied elsewhere. When the risk-based decision field is checked, note the reason in the comment field of the questionnaire and have management review and initial the decision. Additionally, the system security plan for the system should contain supporting documentation as to why the control has or has not been implemented.

The assessor must read each control objective and technique question and determine in partnership with the system owner and those responsible for administering the system, whether the system's sensitivity level warrants the implementation of the control stated in the question. If the control is applicable, check whether there are documented policies (level 1), procedures for implementing the control (level 2), the control has been implemented (level 3), the control has been tested and if found ineffective, remedied (level 4), and whether the control is part of an agency's organizational culture (level 5). The shaded fields in the questionnaire do not require a check mark. The five levels describing the state of the control objective provide a picture of each operational control; however, how well each one of these controls is met is subjective. Criteria have been established for each of the five levels that should be applied when determining whether the control objective has fully reached one or more of the five levels. The criteria are contained in Appendix C, *Federal IT Security Assessment Framework.*

Based on the responses to the control objectives and techniques and in partnership with the system owner and those responsible for system administration, the assessor should conclude the level of the related critical element. The conclusion should consider the relative importance of each subordinate objective/technique to achieving the critical element and the rigor with which the technique is implemented, enforced, and tested.

3.3 Applicability of Control Objectives

As stated above, the critical elements are required to be implemented; the control objectives and techniques, however, tend to be more detailed and leave room for reasonable subjective decisions. If the control does not reasonably apply to the system, then a "non-applicable" or "N/A" can be entered next to the question.

The control objectives and techniques in the questionnaire are geared for a system or group of connected systems. It is possible to use the questionnaire for a program review at an organizational level for ascertaining if the organization has policy and procedures in place (level 1 or level 2). However, to ensure all systems have implemented, tested and fully integrated the controls (level 3, level 4, and level 5), the assessment questionnaire must be applied to each individual or interconnected group of systems. Chapter 4 describes how the results of the assessment can be used as input into an IT security program review.

The policy and procedures for a control objective and technique can be found at the Department level, agency level, agency component level, or application level. To effectively assess a system, ensure that the control objectives being assessed are at the applicable level. For example, if the system being reviewed has stringent authentication procedures, the authentication procedures for the system should be assessed, instead of the agency-wide minimum authentication procedures found in the agency IT security manual.

If a topic area is documented at a high level in policy, the level 1 box should be checked in the questionnaire. If there are additional low level policies for the system, describe the policies in the comment section of the questionnaire. If a specific control is described in detail in procedures, and implemented, the level 2 and level 3 boxes should be checked in the questionnaire. Testing and reviewing controls are an essential part of securing a system. For each specific control, check whether it has been tested and/or reviewed when a significant change occurred. The goal is to have all levels checked for each control. A conceptual sample of completing the questionnaire is contained in Appendix C. The conceptual sample has evolved into the questionnaire and differs slightly, i.e., there is now a comment and initial field.

4. Utilizing the Completed Questionnaire

The questionnaire can be used for two purposes. First it can be used by agency managers who know their agency's systems and security controls to quickly gain a general understanding of where security for a system, group of systems, or the entire agency needs improvement. Second, it can be used as a guide for thoroughly evaluating the status of security for a system. The results of such thorough reviews provide a much more reliable measure of security effectiveness and may be used to 1) fulfill reporting requirements; 2) prepare for audits; and 3) identify resource needs.

4.1 Questionnaire Analysis

Because this is a self-assessment, ideally the individuals assessing the system are the owners of the system or responsible for operating or administering the system. The same individuals who completed the assessment can conduct the analysis of the completed questionnaire. By being familiar with the system, the supporting documentation, and the results of the assessment, the next step that the assessor takes is an analysis, which summarizes the findings. A centralized group, such as an agency's Information System Security Program Office, can also conduct the analysis as long as the supporting documentation is sufficient. The results of the analysis should be placed in an action plan, and the system security plan should be created or updated to reflect each control objective and technique decision.

4.2 Action Plans

How the critical element is to be implemented, i.e., specific procedures written, equipment installed and tested, and personnel trained, should be documented in an action plan. The action plan must contain projected dates, an allocation of resources, and follow-up reviews to ensure that remedial actions have been effective. Routine reports should be submitted to senior management on weaknesses identified, the status of the action plans, and the resources needed.

4.3 Agency IT Security Program Reports

Over the years, agencies have been asked to report on the status of their IT security program. The reporting requests vary in how much detail is required and in the type of information that should be reported. The completed self-assessment questionnaires are a useful resource for compiling agency reports. Below are sample topics that should be considered in an agency-wide security program report:

- Security Program Management
- Management Controls
- Operational Controls
- Technical Controls

- Planned Activities

4.3.1 Security Program Management

An agency's IT security program report needs to address programmatic issues such as:

- an established agency-wide security management structure,
- a documented up-to-date IT security program plan or policy *(The assessment results for level 1 provides input.)*
    - an agency-developed risk management and mitigation plan,
    - an agency-wide incident response capability,
    - an established certification and accreditation policy,
    - an agency-wide anti-virus infrastructure in place and operational at all agency facilities,
    - information security training and awareness programs established and available to all agency employees,
    - roles and relationships clearly defined and established between the agency and bureau levels of information security program management,
- an understanding of the importance of protecting mission critical information assets,
- the integration of security into the capital planning process,
- methods used to ensure that security is an integral part of the enterprise architecture (*The assessment results for the Life Cycle topic area provides input.),*
- the total security cost from this year's budget request and a breakdown of security costs by each major operating division, and
- descriptions of agency-wide guidance issued in the past year.

4.3.2 Management Controls, Operational Controls, and Technical Controls

The results of the completed questionnaires' 17 control topic areas can be used to summarize an agency's implementation of the management, operational, and technical controls. For the report to project an accurate picture, the results must be summarized by system type, not totaled into an overall agency grade level. For example, ten systems were assessed using the questionnaire. Five of the ten systems assessed were major applications; the other five were general support systems. The summary would separate the systems into general support systems and major applications.

By further separating them into groups according to criticality, the report stresses which systems and which control objectives require more attention based on sensitivity and criticality. Not all systems require the same level of protection; the report should reflect that diversity. The use of percentages for describing compliance (i.e., 50 percent of the major applications and 25 percent of general support systems that are high in criticality have complete and current system security plans within the past three years) can be used as long as there is a distinct division provided between the types of systems being reported.

Additionally all or a sampling of the completed questionnaires can be analyzed to determine which controls if implemented would impact the most systems. For example, if viruses frequently plague systems, a stricter firewall policy that prevents attached files in E-mail may be a solution. Also, systemic problems should be culled out. If an agency sees an influx of poor password management controls in the questionnaire results, then possibly password checkers should be used, awareness material issued, and password- aging software installed.

The report should conclude with a summary of planned IT security initiatives. The summary should include goals, actions needed to meet the goals, projected resources, and anticipated dates of completion.

Appendix A

System Questionnaire

Table of Contents

System Name, Title, and Unique Identifier: _____

Major Application _____ **or** **General Support System** _____

Name of Assessors: _____

_____

_____

Date of Evaluation: _____

List of Connected Systems:

Name of System	**Are boundary controls effective?**	**Planned action if not effective**
1.		
2.		
3.		

Criticality of System	Category of Sensitivity High, Medium, or Low
Confidentiality	
Integrity	
Availability	

Purpose and Objective of Assessment: _____

_____

_____

Management Controls

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

1. Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Risk Management *OMB Circular A-130, III*								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? *NIST SP 800-18*								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*								
1.1.3 Has data sensitivity and integrity of the data been considered? *FISCAM SP-1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.4 Have threat sources, both natural and manmade, been identified? *FISCAM SP-1*								
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? *NIST SP 800-30*[2]								
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? *NIST SP 800-30*								
1.2. Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								
1.2.1 Are final risk determinations and related management approvals documented and maintained on file? *FISCAM SP-1*								
1.2.2 Has a mission/business impact analysis been conducted? *NIST SP 800-30*								
1.2.3 Have additional controls been identified to sufficiently mitigate identified risks? *NIST SP 800-30*								

NOTES:

[2] Draft NIST Special Publication 800-30, "Risk Management Guidance" dated June 2001.

2. Review of Security Controls

Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Review of Security Controls *OMB Circular A-130, III* *FISCAM SP-5* *NIST SP 800-18*								
2.1. Critical Element: **Have the security controls of the system and interconnected systems been reviewed?**								
2.1 1 Has the system and all network boundaries been subjected to periodic reviews? *FISCAM SP-5.1*								
2.1.2 Has an independent review been performed when a significant change occurred? *OMB Circular A-130, III* *FISCAM SP-5.1* *NIST SP 800-18*								
2.1.3 Are routine self-assessments conducted ? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? *OMB Circular A-130, 8B3* *NIST SP 800-18*								
2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? *FISCAM SP 3-4* *NIST SP 800-18*								
2.2. Critical Element: **Does management ensure that corrective actions are effectively implemented?**								
2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action? *FISCAM SP 5-1 and 5.2* *NIST SP 800-18*								

NOTES:

3. Life Cycle

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Life Cycle *OMB Circular A-130, III* *FISCAM CC-1.1*								
3.1. Critical Element: **Has a system development life cycle methodology been developed?**								
Initiation Phase								
3.1.1 Is the sensitivity of the system determined? *OMB Circular A-130, III* *FISCAM AC-1.1 & 1.2* *NIST SP 800-18*								
3.1.2 Does the business case document the resources required for adequately securing the system? *Clinger-Cohen*								
3.1.3 Does the Investment Review Board ensure any investment request includes the security resources needed? *Clinger-Cohen*								
3.1.4 Are authorizations for software modifications documented and maintained? *FISCAM CC –1.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.5 Does the budget request include the security resources required for the system? *GISRA*								
Development/Acquisition Phase								
3.1.6 During the system design, are security requirements identified? *NIST SP 800-18*								
3.1.7 Was an initial risk assessment performed to determine security requirements? *NIST SP 800-30*								
3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk? *NIST SP 800-18*								
3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency? *OMB Circular A-130, 8B3*								
3.1.10 Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action? *NIST SP 800-18*								
3.1.11 Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.12 Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented? *NIST SP 800-18*								
Implementation Phase								
3.2. Critical Element: **Are changes controlled as programs progress through testing to final approval?**								
3.2.1 Are design reviews and system tests run prior to placing the system in production? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.2 Are the test results documented? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.3 Is certification testing of security controls conducted and documented? *NIST SP 800-18*								
3.2.4 If security controls were added since development, has the system documentation been modified to include them? *NIST SP 800-18*								
3.2.5 If security controls were added since development, have the security controls been tested and the system recertified? *FISCAM CC-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards? *NIST SP 800-18*								
3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization? *NIST SP 800-18*								
Operation/Maintenance Phase								
3.2.8 Has a system security plan been developed and approved? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? *NIST SP 800-18*								
3.2.10 Is the system security plan kept current? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
Disposal Phase								
3.2.11 Are official electronic records properly disposed/archived? NIST SP 800-18								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? *FISCAM AC-3.4* *NIST SP 800-18*								
3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized? *NIST SP 800-18*								

NOTES:

4. Authorize Processing (Certification & Accreditation)

Authorize processing (Note: Some agencies refer to this process as certification and accreditation) provides a form of assurance of the security of the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Authorize Processing (Certification & Accreditation) *OMB Circular A-130, III* *FIPS 102*								
4.1. Critical Element: **Has the system been certified/recertified and authorized to process (accredited)?**								
4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred? *NIST SP 800-18*								
4.1.2 Has a risk assessment been conducted when a significant change occurred? *NIST SP 800-18*								
4.1.3 Have Rules of Behavior been established and signed by users? *NIST SP 800-18*								
4.1.4 Has a contingency plan been developed and tested? *NIST SP 800-18*								
4.1.5 Has a system security plan been developed, updated, and reviewed? *NIST SP 800-18*								
4.1.6 Are in-place controls operating as intended? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity? *NIST SP 800-18*								
4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? *NIST 800-18*								
4.2. Critical Element: Is the system operating on an interim authority to process in accordance with specified agency procedures?								
4.2.1 Has management initiated prompt action to correct deficiencies? *NIST SP 800-18*								

NOTES:

5. System Security Plan

System security plans provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan delineates responsibilities and expected behavior of all individuals who access the system. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
System security plan *OMB Circular A-130, III* *NIST SP 800-18* *FISCAM SP-2.1*								
5.1. Critical Element: **Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?**								
5.1.1 Is the system security plan approved by key affected parties and management? *FISCAM SP-2.1* *NIST SP 800-18*								
5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? *NIST SP 800-18*								
5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? *OMB Circular A-130, III* *NIST SP 800-18*								
5.2. Critical Element: **Is the plan kept current?**								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks? *FISCAM SP-2.1* *NIST SP 800-18*								

NOTES:

Operational Controls

The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

6. Personnel Security

Many important issues in computer security involve human users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Personnel Security *OMB Circular A-130, III*								
6.1. Critical Element: **Are duties separated to ensure least privilege and individual accountability?**								
6.1.1 Are all positions reviewed for sensitivity level? *FISCAM SD-1.2* *NIST SP 800-18*								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? *FISCAM SD-1.2*								
6.1.3 Are sensitive functions divided among different individuals? *OMB Circular A-130, III* *FISCAM SD-1* *NIST SP 800-18*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1.4 Are distinct systems support functions performed by different individuals? *FISCAM SD-1.1*								
6.1.5 Are mechanisms in place for holding users responsible for their actions? *OMB Circular A-130, III* *FISCAM SD-2 & 3.2*								
6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required? *FISCAM SD-1.1* *FISCAM SP-4.1*								
6.1.7 Are hiring, transfer, and termination procedures established? *FISCAM SP-4.1* *NIST SP 800-18*								
6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? *FISCAM SP-4.1* *NIST 800-18*								
6.2. Critical Element: Is appropriate background screening for assigned positions completed prior to granting access?								
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? *OMB Circular A-130, III* *FISCAM SP-4.1*								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? *FISCAM SP-4.1*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? *OMB Circular A-130, III*								
6.2.4 Are there conditions for allowing system access prior to completion of screening? *FISCAM AC-2.2* *NIST SP 800-18*								

NOTES:

7. Physical and Environmental Protection

Physical security and environmental security are the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Physical and Environmental Protection								
Physical Access Control								
7.1. Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?								
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics? *FISCAM AC-3 NIST SP 800-18*								
7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities? *FISCAM AC-3.1*								
7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? *FISCAM AC-3.1*								
7.1.4 Are keys or other access devices needed to enter the computer room and tape/media library? *FISCAM AC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.5 Are unused keys or other entry devices secured? *FISCAM AC-3.1*								
7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc? *FISCAM AC-3.1*								
7.1.7 Are visitors to sensitive areas signed in and escorted? *FISCAM AC-3.1*								
7.1.8 Are entry codes changed periodically? *FISCAM AC-3.1*								
7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? *FISCAM AC-4*								
7.1.10 Is suspicious access activity investigated and appropriate action taken? *FISCAM AC-4.3*								
7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? *FISCAM AC-3.1*								
Fire Safety Factors								
7.1.12 Are appropriate fire suppression and prevention devices installed and working? *FISCAM SC-2.2* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.13 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically? *NIST SP 800-18*								
Supporting Utilities								
7.1.14 Are heating and air-conditioning systems regularly maintained? *NIST SP 800-18*								
7.1.15 Is there a redundant air-cooling system? *FISCAM SC-2.2*								
7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.17 Are building plumbing lines known and do not endanger system? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.18 Has an uninterruptible power supply or backup generator been provided? *FISCAM SC-2.2*								
7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.? *FISCAM SC-2.2*								
Interception of Data								
7.2. Critical Element: Is data protected from interception?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? *NIST SP 800-18*								
7.2.2 Is physical access to data transmission lines controlled? *NIST SP 800-18*								
Mobile and Portable Systems								
7.3. Critical Element: Are mobile and portable systems protected?								
7.3.1 Are sensitive data files encrypted on all portable systems? *NIST SP 800-14*								
7.3.2 Are portable systems stored securely? *NIST SP 800-14*								

NOTES:

8. Production, Input/Output Controls

There are many aspects to supporting IT operations. Topics range from a user help desk to procedures for storing, handling and destroying media. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Production, Input/Output Controls								
8.1. Critical Element: Is there user support?								
8.1.1 Is there a help desk or group that offers advice? *NIST SP 800-18*								
8.2. Critical Element: Are there media controls?								
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? *NIST SP 800-18*								
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media? *NIST SP 800-18*								
8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? *NIST SP 800-18*								
8.2.4 Are controls in place for transporting or mailing media or printed output? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
8.2.5 Is there internal/external labeling for sensitivity? *NIST SP 800-18*								
8.2.6 Is there external labeling with special handling instructions? *NIST SP 800-18*								
8.2.7 Are audit trails kept for inventory management? *NIST SP 800-18*								
8.2.8 Is media sanitized for reuse? *FISCAM AC-3.4* *NIST SP 800-18*								
8.2.9 Is damaged media stored and /or destroyed? *NIST SP 800-18*								
8.2.10 Is hardcopy media shredded or destroyed when no longer needed? *NIST SP 800-18*								

NOTES:

9. Contingency Planning

Contingency planning involves more than planning for a move offsite after a disaster destroys a facility. It also addresses how to keep an organization's critical functions operating in the event of disruptions, large and small. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Contingency Planning *OMB Circular A-130, III*								
9.1. Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?								
9.1.1 Are critical data files and operations identified and the frequency of file backup documented? *FISCAM SC- SC-1.1 & 3.1 NIST SP 800-18*								
9.1.2 Are resources supporting critical operations identified? *FISCAM SC-1.2*								
9.1.3 Have processing priorities been established and approved by management? *FISCAM SC-1.3*								
9.2. Critical Element: Has a comprehensive contingency plan been developed and documented?								
9.2.1 Is the plan approved by key affected parties? *FISCAM SC-3.1*								
9.2.2 Are responsibilities for recovery assigned? *FISCAM SC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.2.3 Are there detailed instructions for restoring operations? *FISCAM SC-3.1*								
9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place? *FISCAM SC-3.1* *NIST SP 800-18*								
9.2.5 Is the location of stored backups identified? *NIST SP 800-18*								
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? *FISCAM SC-2.1*								
9.2.7 Is system and application documentation maintained at the off-site location? *FISCAM SC-2.1*								
9.2.8 Are all system defaults reset after being restored from a backup? *FISCAM SC-3.1*								
9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? *FISCAM SC-2.1*								
9.2.10 Has the contingency plan been distributed to all appropriate personnel? *FISCAM SC-3.1*								
9.3. Critical Element: Are tested contingency/disaster recovery plans in place?								
9.3.1 Is an up-to-date copy of the plan stored securely off-site? *FISCAM SC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.3.2 Are employees trained in their roles and responsibilities? *FISCAM SC-2.3* *NIST SP 800-18*								
9.3.3 Is the plan periodically tested and readjusted as appropriate? *FISCAM SC-3.1* *NIST SP 800-18*								

NOTES:

10. Hardware and System Software Maintenance

These are controls used to monitor the installation of, and updates to, hardware and software to ensure that the system functions as expected and that a historical record is maintained of changes. Some of these controls are also covered in the Life Cycle Section. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Hardware and System Software Maintenance *OMB Circular A-130, III*								
10.1. Critical Element: Is access limited to system software and hardware?								
10.1.1 Are restrictions in place on who performs maintenance and repair activities? *OMB Circular A-130, III* *FISCAM SS-3.1* *NIST SP 800-18*								
10.1.2 Is access to all program libraries restricted and controlled? *FISCAM CC-3.2 & 3.3*								
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)? *NIST SP 800-18*								
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls? *FISCAM SS-1.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities? *FISCAM SS-2.1*								
10.2. Critical Element: Are all new and revised hardware and software authorized, tested and approved before implementation?								
10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control? *NIST SP 800-18*								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production? *FISCAM SS-3.1, 3.2, & CC-2.1* *NIST SP 800-18*								
10.2.3 Are software change request forms used to document requests and related approvals? *FISCAM CC-1.2* *NIST SP 800-18*								
10.2..4 Are there detailed system specifications prepared and reviewed by management? *FISCAM CC-2.1*								
10.2.5 Is the type of test data to be used specified, i.e., live or made up? *NIST SP 800-18*								
10.2.6 Are default settings of security features set to the most restrictive mode? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.7 Are there software distribution implementation orders including effective date provided to all locations? *FISCAM CC-2.3*								
10.2.8 Is there version control? *NIST SP 800-18*								
10.2.9 Are programs labeled and inventoried? *FISCAM CC-3.1*								
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed? *FISCAM SS-3.2*								
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact? *FISCAM CC-2.2*								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes? *FISCAM SC-2.1* *NIST SP 800-18*								
10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented? *NIST SP 800-18*								
10.3. Are systems managed to reduce vulnerabilities?								
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed? *NIST SP 800-18*								

NOTES:

11. Data Integrity

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user the information meets expectations about its quality and integrity. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Data Integrity *OMB Circular A-130, 8B3*								
11.1. Critical Element: Is virus detection and elimination software installed and activated?								
11.1.1 Are virus signature files routinely updated? *NIST SP 800-18*								
11.1.2 Are virus scans automatic? *NIST SP 800-18*								
11.2. Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?								
11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? *NIST SP 800-18*								
11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken? *FISCAM SS-2.2*								
11.2.3 Are procedures in place to determine compliance with password policies? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? *NIST SP 800-18*								
11.2.5 Are intrusion detection tools installed on the system? *NIST SP 800-18*								
11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? *NIST SP 800-18*								
11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks? *NIST SP 800-18*								
11.2.8 Is penetration testing performed on the system? *NIST SP 800-18*								
11.2.9 Is message authentication used? *NIST SP 800-18*								

NOTES:

12. Documentation

The documentation contains descriptions of the hardware, software, policies, standards, procedures, and approvals related to the system and formalize the system's security controls. When answering whether there are procedures for each control objective, the question should be phrased "are there procedures for ensuring the documentation is obtained and maintained." The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Documentation *OMB Circular A-130, 8B3*								
12.1. Critical Element: **Is there sufficient documentation that explains how software/hardware is to be used?**								
12.1.1 Is there vendor-supplied documentation of purchased software? *NIST SP 800-18*								
12.1.2 Is there vendor-supplied documentation of purchased hardware? *NIST SP 800-18*								
12.1.3 Is there application documentation for in-house applications? *NIST SP 800-18*								
12.1.4 Are there network diagrams and documentation on setups of routers and switches? *NIST SP 800-18*								
12.1.5 Are there software and hardware testing procedures and results? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.1.6 Are there standard operating procedures for all the topic areas covered in this document? *NIST SP 800-18*								
12.1.7 Are there user manuals? *NIST SP 800-18*								
12.1.8 Are there emergency procedures? *NIST SP 800-18*								
12.1.9 Are there backup procedures? *NIST SP 800-18*								
12.2. Critical Element: **Are there formal security and operational procedures documented?**								
12.2.1 Is there a system security plan? *OMB Circular A-130, III* *FISCAM SP-2.1* *NIST SP 800-18*								
12.2.2 Is there a contingency plan? *NIST SP 800-18*								
12.2.3 Are there written agreements regarding how data is shared between interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
12.2.4 Are there risk assessment reports? *NIST SP 800-18*								
12.2.5 Are there certification and accreditation documents and a statement authorizing the system to process? *NIST SP 800-18*								

NOTES:

13. Security Awareness, Training, and Education

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Security awareness, training, and education enhance security by improving awareness of the need to protect system resources. Additionally, training develops skills and knowledge so computer users can perform their jobs more securely and build in-depth knowledge. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Security Awareness, Training, and Education *OMB Circular A-130, III*								
13.1. Critical Element: Have employees received adequate training to fulfill their security responsibilities?								
13.1.1 Have employees received a copy of the Rules of Behavior? *NIST SP 800-18*								
13.1.2 Are employee training and professional development documented and monitored? *FISCAM SP-4.2*								
13.1.3 Is there mandatory annual refresher training? *OMB Circular A-130, III*								
13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets? *NIST SP 800-18*								
13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? *NIST SP 800-18*								

NOTES:

14. Incident Response Capability

Computer security incidents are an adverse event in a computer system or network. Such incidents are becoming more common and their impact far-reaching. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Incident Response Capability *OMB Circular A-130, III* *FISCAM SP-3.4* *NIST 800-18*								
14.1. Critical Element: **Is there a capability to provide help to users when a security incident occurs in the system?**								
14.1.1 Is a formal incident response capability available? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.2 Is there a process for reporting incidents? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.3 Are incidents monitored and tracked until resolved? *NIST SP 800-18*								
14.1.4 Are personnel trained to recognize and handle incidents? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.5 Are alerts/advisories received and responded to? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs? *NIST SP 800-18*								
14.2. Critical Element: **Is incident related information shared with appropriate organizations?**								
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
14.2.2 Is incident information shared with FedCIRC[3] concerning incidents and common vulnerabilities and threats? *OMB A-130, III* *GISRA*								
14.2.3 Is incident information reported to FedCIRC, NIPC[4], and local law enforcement when necessary? *OMB A-130,III* *GISRA*								

[3] FedCIRC (Federal Computer Incident Response Capability) is the U.S. Government's focal point for handling computer security-related incidents.

[4] NIPC's mission is to serve as the U.S. Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures.

NOTES:

Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

15. Identification and Authentication

Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. The following questions are organized according to two critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Identification and Authentication *OMB Circular A-130, III* *FISCAM AC-2* *NIST SP 800-18*								
15.1. Critical Element: **Are users individually authenticated via passwords, tokens, or other devices?**								
15.1.1 Is a current list maintained and approved of authorized users and their access? *FISCAM AC-2* *NIST SP 800-18*								
15.1.2 Are digital signatures used and conform to FIPS 186-2? *NIST SP 800-18*								
15.1.3 Are access scripts with embedded passwords prohibited? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.4 Is emergency and temporary access authorized? *FISCAM AC-2.2*								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? *FISCAM AC-3.2*								
15.1.6 Are passwords changed at least every ninety days or earlier if needed? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.8 Are inactive user identifications disabled after a specified period of time? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.9 Are passwords not displayed when entered? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.10 Are there procedures in place for handling lost and compromised passwords? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.12 Are passwords transmitted and stored using secure protocols/algorithms? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.13 Are vendor-supplied passwords replaced immediately? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user? *FISCAM AC-3.2* *NIST SP 800-18*								
15.2. Critical Element: **Are access controls enforcing segregation of duties?**								
15.2.1 Does the system correlate actions to users? *OMB A-130, III* *FISCAM SD-2.1*								
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate? *FISCAM AC-2.1*								

NOTES:

16. Logical Access Controls

Logical access controls are the system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. The following questions are organized according to three critical elements. The levels for each of these critical elements should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Logical Access Controls *OMB Circular A-130, III* *FISCAM AC-3.2* *NIST SP 800-18*								
16.1. Critical Element: **Do the logical access controls restrict users to authorized transactions and functions?**								
16.1.1 Can the security controls detect unauthorized access attempts? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.3 Is access to security software restricted to security administrators? *FISCAM AC-3.2*								
16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity? *FISCAM AC-3.2* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.5 Are inactive users' accounts monitored and removed when not needed? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.7 If encryption is used, does it meet federal standards? *NIST SP 800-18*								
16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? *NIST SP 800-18*								
16.1.9 Is access restricted to files at the logical view or field? *FISCAM AC-3.2*								
16.1.10 Is access monitored to identify apparent security violations and are such events investigated? *FISCAM AC-4*								
16.2. Critical Element: **Are there logical controls over network access?**								
16.2.1 Has communication software been implemented to restrict access through specific terminals? *FISCAM AC-3.2*								
16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings? *PSN Security Assessment Guidelines*								
16.2.4 Are there controls that restrict remote access to the system? *NIST SP 800-18*								
16.2.5 Are network activity logs maintained and reviewed? *FISCAM AC-3.2*								
16.2.6 Does the network connection automatically disconnect at the end of a session? *FISCAM AC-3.2*								
16.2.7 Are trust relationships among hosts and external entities appropriately restricted? *PSN Security Assessment Guidelines*								
16.2.8 Is dial-in access monitored? *FISCAM AC-3.2*								
16.2.9 Is access to telecommunications hardware or facilities restricted and monitored? *FISCAM AC-3.2*								
16.2.10 Are firewalls or secure gateways installed? *NIST SP 800-18*								
16.2.11 If firewalls are installed do they comply with firewall policy and rules? *FISCAM AC-3.2*								
16.2.12 Are guest and anonymous accounts authorized and monitored? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.13 Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished? *FISCAM AC-3.2* *NIST SP 800-18*								
16.2.14 Are sensitive data transmissions encrypted? *FISCAM AC-3.2*								
16.2.15 Is access to tables defining network options, resources, and operator profiles restricted? *FISCAM AC-3.2*								
16.3. Critical Element: **If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?**								
16.3.1 Is a privacy policy posted on the web site? *OMB-99-18*								

NOTES:

17. Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. The following questions are organized under one critical element. The levels for the critical element should be determined based on the answers to the subordinate questions.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Audit Trails *OMB Circular A-130, III* *FISCAM AC-4.1* *NIST SP 800-18*								
17.1. Critical Element: **Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?**								
17.1.1 Does the audit trail provide a trace of user actions? *NIST SP 800-18*								
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? *NIST SP 800-18*								
17.1.3 Is access to online audit logs strictly controlled? *NIST SP 800-18*								
17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? *NIST SP 800-18*								
17.1.6 Are audit trails reviewed frequently? *NIST SP 800-18*								
17.1.7 Are automated tools used to review audit records in real time or near real time? *NIST SP 800-18*								
17.1.8 Is suspicious activity investigated and appropriate action taken? *FISCAM AC-4.3*								
17.1.9 Is keystroke monitoring used? If so, are users notified? *NIST SP 800-18*								

NOTES:

Appendix B – Source of Control Criteria

Office of Management and Budget Circular A-130, "Management of Federal Information Resources", Section 8B3 and Appendix III, "Security of Federal Automated Information Resources."	Establishes a minimum set of controls to be included in Federal IT security programs.
Computer Security Act of 1987.	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995.	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996.	This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
Presidential Decision Directive 63, "Protecting America's Critical Infrastructures."	This directive specifies agency responsibilities for protecting the nation's infrastructure, assessing vulnerabilities of public and private sectors, and eliminating vulnerabilities.
OMB Memorandum 99-18, "Privacy Policies on Federal Web Sites."	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
General Accounting Office "Federal Information System Control Audit Manual" (FISCAM).	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Security Information Technology Systems."	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.
NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."	This publication details the specific controls that should be documented in a system security plan.
Defense Authorization Act (P.L. 106-398) including Title X, Subtitle G, "Government Information Security Reform" (GISRA)	The act primarily addresses the program management and evaluation aspects of security.
Office of the Manager, National Communications Systems, "Public Switched Network Security Assessment Guidelines."	The guide describes a risk assessment procedure, descriptions of a comprehensive security program, and a summary checklist.
Federal Information Processing Standards.	These documents contain mandates and/or guidance for improving the utilization and management of computers and IT systems in the Federal Government.

Federal Information Technology Security Assessment Framework

November 28, 2000

Prepared for

Security, Privacy, and Critical Infrastructure Committee

by

National Institute of Standards and Technology (NIST)
Computer Security Division

Overview

Information and the systems that process it are among the most valuable assets of any organization. Adequate security of these assets is a fundamental management responsibility. Consistent with Office of Management and Budget (OMB) policy, each agency must implement and maintain a program to adequately secure its information and system assets. Agency programs must: 1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability; and 2) protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification.

Agencies must plan for security, and ensure that the appropriate officials are assigned security responsibility and authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible agency officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

The Federal Information Technology (IT) Security Assessment Framework (or Framework) provides a method for agency officials to 1) determine the current status of their security programs relative to existing policy and 2) where necessary, establish a target for improvement. It does not establish new security requirements. The Framework may be used to assess the status of security controls for a given asset or collection of assets. These assets include information, individual systems (e.g., major applications, general support systems, mission critical systems), or a logically related grouping of systems that support operational programs, or operational programs (e.g., Air Traffic Control, Medicare, Student Aid). Assessing all asset security controls and all interconnected systems that the asset depends on produces a picture of both the security condition of an agency component and of the entire agency.

The Framework comprises five levels to guide agency assessment of their security programs and assist in prioritizing efforts for improvement. Coupled with the NIST-prepared self-assessment questionnaire[5], the Framework provides a vehicle for consistent and effective measurement of the security status for a given asset. The security status is measured by determining if specific security controls are documented, implemented, tested and reviewed, and incorporated into a cyclical review/improvement program, as well as whether unacceptable risks are identified and mitigated. The NIST questionnaire provides specific questions that identify the control criteria against which agency policies, procedures, and security controls can be compared. Appendix A contains a sample of the upcoming NIST Special Publication.

The Framework is divided into five levels: Level 1 of the Framework reflects that an asset has documented security policy. At level 2, the asset also has documented procedures and controls to implement the policy. Level 3 indicates that procedures and controls have been implemented. Level 4 shows that the procedures and controls are tested and reviewed. At level 5, the asset has procedures and controls fully integrated into a comprehensive program.

[5] The NIST Self-assessment Questionnaire will be issued in 2001 as a NIST Special Publication.

Each level represents a more complete and effective security program. OMB and the Council recognize that the security needs for the tens of thousands of Federal information systems differ. Agencies should note that testing the effectiveness of the asset and all interconnected systems that the asset depends on is essential to understanding whether risk has been properly mitigated. When an individual system does not achieve level 4, agencies should determine whether that system meets the criteria found in OMB Memorandum M00-07 (February 28, 2000) "Incorporating and Funding Security in Information Systems Investments." Agencies should seek to bring all assets to level 4 and ultimately level 5.

Integral to all security programs whether for an asset or an entire agency is a risk assessment process that includes determining the level of sensitivity of information and systems. Many agencies have developed their own methods of making these determinations. For example, the Department of Health and Human Services uses a four--track scale for confidentiality, integrity, and availability. The Department of Energy uses five groupings or "clusters" to address sensitivity. Regardless of the method used, the asset owner is responsible for determining how sensitive the asset is, what level of risk is acceptable, and which specific controls are necessary to provide adequate security to that asset. Again, each implemented security control must be periodically tested for effectiveness. The decision to implement and the results of the testing should be documented.

1. Framework Description

The Federal Information Technology Security Assessment Framework (Framework) identifies five levels of IT security program effectiveness (see Figure 1). The five levels measure specific management, operational, and technical control objectives. Each of the five levels contains criteria to determine if the level is adequately implemented. For example, in Level 1, all written policy should contain the purpose and scope of the policy, the individual(s) responsible for implementing the policy, and the consequences and penalties for not following the policy. The policy for an individual control must be reviewed to ascertain that the criteria for level 1 are met. Assessing the effectiveness of the individual controls, not simply their existence, is key to achieving and maintaining adequate security.

The asset owner, in partnership with those responsible for administering the information assets (which include IT systems), must determine whether the measurement criteria are being met at each level. Before making such a determination, the degree of sensitivity of information and systems must be determined by considering the requirements for confidentiality, integrity, and availability of both the information and systems -- the value of information and systems is one of the major factors in risk management.

A security program may be assessed at various levels within an organization. For example, a program could be defined as an agency asset, a major application, general support system, high impact program, physical plant, mission critical system, or logically related group of systems. The Framework refers to this grouping as an asset.

The Framework describes an asset self-assessment and provides levels to guide and prioritize agency efforts as well as a basis to measure progress. In addition, the National Institute of Standards and Technology (NIST) will develop a questionnaire that gives the implementation tools for the Framework. The questionnaire will contain specific control objectives that should be applied to secure a system.

Figure 1 – Federal IT Security Assessment Framework

Level 1	Documented Policy
Level 2	Documented Procedures
Level 3	Implemented Procedures and Controls
Level 4	Tested and Reviewed Procedures and Controls
Level 5	Fully Integrated Procedures and Controls

The Framework approach begins with the premise that all agency assets must meet the minimum security requirements of the Office of Management and Budget Circular A-130, "Management of Federal Resources", Appendix III, "Security of Federal Automated Information Resources" (A-130). The criteria that are outlined in the Framework and provided in detail in the questionnaire are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy. It should be noted that an agency might have additional laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability. Each agency should decide if additional security controls should be added to the questionnaire and, if so, customize the questionnaire appropriately. A list of the documents that the Framework and the questionnaire draw upon is provided in Figure 2.

Figure 2 – Source of Control Criteria

Office of Management and Budget Circular A-130, "Management of Federal Information Resources", Appendix III, "Security of Federal Automated Information Resources."	Establishes a minimum set of controls to be included in Federal IT security programs.
Computer Security Act of 1987.	This statute set the stage for protecting systems by codifying the requirement for Government-wide IT security planning and training.
Paperwork Reduction Act of 1995.	The PRA established a comprehensive information resources management framework including security and subsumed the security responsibilities of the Computer Security Act of 1987.
Clinger-Cohen Act of 1996.	This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.
Presidential Decision Directive 63, "Protecting America's Critical Infrastructures."	This directive specifies agency responsibilities for protecting the nation's infrastructure, assessing vulnerabilities of public and private sectors, and eliminating vulnerabilities.
Presidential Decision Directive 67, "Enduring Constitutional Government and Continuity of Government."	Relates to ensuring constitutional government, continuity of operations (COOP) planning, and continuity of government (COG) operations
OMB Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records."	This memorandum provides instructions to agencies on how to comply with the President's Memorandum of May 14, 1998 on "Privacy and Personal Information in Federal Records."
OMB Memorandum 99-18, "Privacy Policies on Federal Web Sites."	This memorandum directs Departments and Agencies to post clear privacy policies on World Wide Web sites, and provides guidance for doing so.
OMB Memorandum 00-13, "Privacy Policies and Data Collection on Federal Web Sites."	The purpose of this memorandum is a reminder that each agency is required by law and policy to establish clear privacy policies for its web activities and to comply with those policies.
General Accounting Office "Federal Information System Control Audit Manual" (FISCAM).	The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.
NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Security Information Technology Systems."	This publication guides organizations on the types of controls, objectives, and procedures that comprise an effective security program.
NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems."	This publication details the specific controls that should be documented in a system security plan.
Federal Information Processing Standards.	This document contains legislative and executive mandates for improving the utilization and management of computers and IT systems in the Federal Government.

2. Documented Policy - Level 1

2.1 Description

Level 1 of the Framework includes:

- Formally documented and disseminated security policy covering agency headquarters and major components (e.g., bureaus and operating divisions). The policy may be asset specific.
- Policy that references most of the basic requirements and guidance issued from the documents listed in Figure 2 – Source of Control Criteria.

An asset is at level 1 if there is a formally, up-to-date documented policy that establishes a continuing cycle of assessing risk, implements effective security policies including training, and uses monitoring for program effectiveness. Such a policy may include major agency components, (e.g., bureaus and operating divisions) or specific assets.

A documented security policy is necessary to ensure adequate and cost effective organizational and system security controls. A sound policy delineates the security management structure and clearly assigns security responsibilities, and lays the foundation necessary to reliably measure progress and compliance. The criteria listed below should be applied when assessing the policy developed for the controls that are listed in the NIST questionnaire.

2.2 Criteria

Level 1 criteria describe the components of a security policy.

Criteria for Level 1
a. Purpose and scope. An up-to-date security policy is written that covers all major facilities and operations agency-wide or for the asset. The policy is approved by key affected parties and covers security planning, risk management, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The policy clearly identifies the purpose of the program and its scope within the organization.
b. Responsibilities. The security program comprises a security management structure with adequate authority, and expertise. IT security manager(s) are appointed at an overall level and at appropriate subordinate levels. Security responsibilities and expected behaviors are clearly defined for asset owners and users, information resources management and data processing personnel, senior management, and security administrators.
c. Compliance. General compliance and specified penalties and disciplinary actions are also identified in the policy.

3. Documented Procedures - Level 2

3.1 Description

Level 2 of the Framework includes:

- Formal, complete, well-documented procedures for implementing policies established at level one.
- The basic requirements and guidance issued from the documents listed in Figure 2 – Source of Control Criteria.

An asset is at level 2 when formally documented procedures are developed that focus on implementing specific security controls. Formal procedures promote the continuity of the security program. Formal procedures also provide the foundation for a clear, accurate, and complete understanding of the program implementation. An understanding of the risks and related results should guide the strength of the control and the corresponding procedures. The procedures document the implementation of and the rigor in which the control is applied. Level 2 requires procedures for a continuing cycle of assessing risk and vulnerabilities, implementing effective security policies, and monitoring effectiveness of the security controls. Approved system security plans are in place for all assets.

Well-documented and current security procedures are necessary to ensure that adequate and cost effective security controls are implemented. The criteria listed below should be applied when assessing the quality of the procedures for controls outlined in the NIST questionnaire.

3.2 Criteria

Level 2 criteria describe the components of security procedures.

Criteria for Level 2
a. Control areas listed and organization's position stated. Up-to-date procedures are written that covers all major facilities and operations within the asset. The procedures are approved by key responsible parties and cover security policies, security plans, risk management, review of security controls, rules of behavior, life-cycle management, processing authorization, personnel, physical and environmental aspects, computer support and operations, contingency planning, documentation, training, incident response, access controls, and audit trails. The procedures clearly identify management's position and whether there are further guidelines or exceptions.
b. Applicability of procedures documented. Procedures clarify where, how, when, to, whom, and about what a particular procedure applies.
c. Assignment of IT security responsibilities and expected behavior. Procedures clearly define security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and data processing personnel, (3) management, and (4) security administrators.
d. Points of contact and supplementary information provided. Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance.

4. Implemented Procedures and Controls - Level 3

4.1 Description

Level 3 of the Framework includes:

- Security procedures and controls that are implemented.
- Procedures that are communicated and individuals who are required to follow them.

At level 3, the IT security procedures and controls are implemented in a consistent manner and reinforced through training. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. Security controls for an asset could be implemented and not have procedures documented, but the addition of formal documented procedures at level 2 represents a significant step in the effectiveness of implementing procedures and controls at level 3. While testing the on-going effectiveness is not emphasized in level 3, some testing is needed when initially implementing controls to ensure they are operating as intended. The criteria listed below should be used to determine if the specific controls listed in the NIST questionnaire are being implemented.

4.2 Criteria

Level 3 criteria describe how an organization can ensure implementation of their security procedures.

Criteria for Level 3
a. Owners and users are made aware of security policies and procedures. Security policies and procedures are distributed to all affected personnel, including system/application rules and expected behaviors. Requires users to periodically acknowledge their awareness and acceptance of responsibility for security.
b. Policies and procedures are formally adopted and technical controls installed. Automated and other tools routinely monitor security. Established policy governs review of system logs, penetration testing, and internal/external audits.
c. Security is managed throughout the life cycle of the system. Security is considered in each of the life-cycle phases: initiation, development/acquisition, implementation, operation, and disposal.
d. Procedures established for authorizing processing (certification and accreditation). Management officials must formally authorize system operations and manage risk.
e. Documented security position descriptions. Skill needs and security responsibilities in job descriptions are accurately identified.
f. Employees trained on security procedures. An effective training and awareness program tailored for varying job functions is planned, implemented, maintained, and evaluated.

5. Tested and Evaluated Procedures and Controls - Level 4

5.1 Description

Level 4 of the Framework includes:

- Routinely evaluating the adequacy and effectiveness of security policies, procedures, and controls.

- Ensuring that effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual security incidents or through security alerts issued by FedCIRC, vendors, and other trusted sources.

Routine evaluations and response to identified vulnerabilities are important elements of risk management, which includes identifying, acknowledging, and responding, as appropriate, to changes in risk factors (e.g., computing environment, data sensitivity) and ensuring that security policies and procedures are appropriate and are operating as intended on an ongoing basis.

Routine self-assessments are an important means of identifying inappropriate or ineffective security procedures and controls, reminding employees of their security-related responsibilities, and demonstrating management's commitment to security. Self-assessments can be performed by agency staff or by contractors or others engaged by agency management. Independent audits such as those arranged by the General Accounting Office (GAO) or an agency Inspector General (IG), are an important check on agency performance, but should not be viewed as a substitute for evaluations initiated by agency management.

To be effective, routine evaluations must include tests and examinations of key controls. Reviews of documentation, walk-throughs of agency facilities, and interviews with agency personnel, while providing useful information, are not sufficient to ensure that controls, especially computer-based controls, are operating effectively. Examples of tests that should be conducted are network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing). Tests performed should consider the risks of authorized users exceeding authorization as well as unauthorized users (e.g., external parties, hackers) gaining access. Similar to levels 1 through 3, to be meaningful, evaluations must include security controls of interconnected assets, e.g., network supporting applications being tested.

When assets are first implemented or are modified, they should be tested and certified to ensure that controls are initially operating as intended. (This would occur at Level 3.) Requirements for subsequent testing and recertification should be integrated into an agency's ongoing test and evaluation program.

In addition to test results, agency evaluations should consider information gleaned from records of potential and actual security incidents and from security alerts, such as those issued by software vendors. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risks.

The criteria listed below should be applied to each control area listed in the NIST questionnaire to determine if the asset is being effectively evaluated.

5.2 Criteria

Level 4 criteria are listed below.

Criteria for Level 4
a. Effective program for evaluating adequacy and effectiveness of security policies, procedures, and controls. Evaluation requirements, including requirements regarding the type and frequency of testing, should be documented, approved, and effectively implemented. The frequency and rigor with which individual controls are tested should depend on the risks that will be posed if the controls are not operating effectively. At a minimum, controls should be evaluated whenever significant system changes are made or when other risk factors, such as the sensitivity of data processed, change. Even controls for inherently low-risk operations should be tested at a minimum of every 3 years.
b. Mechanisms for identifying vulnerabilities revealed by security incidents or security alerts. Agencies should routinely analyze security incident records, including any records of anomalous or suspicious activity that may reveal security vulnerabilities. In addition, they should review security alerts issued by FedCIRC, vendors, and others.
c. Process for reporting significant security weaknesses and ensuring effective remedial action. *Such a process should provide for routine reports to senior management on weaknesses identified through testing or other means, development of action plans, allocation of needed resources, and follow-up reviews to ensure that remedial actions have been effective. Expedited processes should be implemented for especially significant weaknesses that may present undue risk if not addressed immediately.*

6. Fully Integrated Procedures and Controls - Level 5

6.1 Description

Level 5 of the Framework includes:

- A comprehensive security program that is an integral part of an agency's organizational culture.

- Decision-making based on cost, risk, and mission impact.

The consideration of IT security is pervasive in the culture of a level 5 asset. A proven life-cycle methodology is implemented and enforced and an ongoing program to identify and institutionalize best practices has been implemented. There is active support from senior management. Decisions and actions that are part of the IT life cycle include:

- Improving security program
- Improving security program procedures
- Improving or refining security controls
- Adding security controls
- Integrating security within existing and evolving IT architecture
- Improving mission processes and risk management activities

Each of these decisions result from a continuous improvement and refinement program instilled within the organization. At level 5, the understanding of mission-related risks and the associated costs of reducing these risks are considered with a full range of implementation options to achieve maximum mission cost-effectiveness of security measures. Entities should apply the principle of selecting controls that offer the lowest cost implementation while offering adequate risk mitigation, versus high cost implementation and low risk mitigation. The criteria listed below should be used to assess whether a specific control contained in the NIST questionnaire has been fully implemented.

6.2 Criteria

Level 5 criteria describe components of a fully integrated security program.

Criteria for Level 5
a. There is an active enterprise-wide security program that achieves cost-effective security.
b. IT security is an integrated practice within the asset.
c. Security vulnerabilities are understood and managed.
d. Threats are continually re-evaluated, and controls adapted to changing security environment.
e. Additional or more cost-effective security alternatives are identified as the need arises.
f. Costs and benefits of security are measured as precisely as practicable.
g. Status metrics for the security program are established and met.

7. Future of the Framework

This version of the Framework primarily addresses security management issues. It describes a process for agencies to assess their compliance with long-standing basic requirements and guidance. With the Framework in place, agencies will have an approach to begin the assessment process. The NIST questionnaire provides the tool to determine whether agencies are meeting these requirements and following the guidance.

The Framework is not static; it is a living document. Revisions will focus on expanding, refining, and providing more granularity for existing criteria. In addition, the establishment of a similar companion framework devoted to the evolution of agency electronic privacy polices may be considered in time.

The Framework can be viewed as both an auditing tool and a management tool.
A balance between operational needs and cost effective security for acceptable risk will need to be made to achieve an adequate level of security.

Currently, the NIST self-assessment tool is under development and will be available in 2001. Appendix A provides a sample questionnaire to assist agencies until NIST officially releases the questionnaire.

Appendix A
Conceptual Sample of NIST Self-Assessment Questionnaire

Below is a conceptual sample of the Hypothetical Government Agency's (HGA) completion of the NIST questionnaire for their Training Database. Before the questionnaire was completed, the sensitivity of the information stored within, processed by and transmitted by this asset was assessed. The premise behind determining the level of sensitivity is that each asset owner is responsible for determining what level of risk is acceptable, and which specific security controls are necessary to provide adequate security.

The sensitivity of this asset was determined to be high for confidentiality and low for integrity and availability. The confidentiality of the system is high due to the system containing personnel information. Employee social security numbers, course lists, and grades are contained in the system. The integrity of the database is considered low because if the information were modified by unauthorized, unanticipated or unintentional means, employees, who can read their own training file, would detect the modifications. The availability of the system is considered low because hard copies of the training forms are available as a backup.

The questionnaire was completed for the database with the understanding that security controls that protect the integrity or availability of the data did not have to be rigidly applied. The questionnaire contains a field that can be checked when a risk-based decision has been made to either reduce or enhance a security control. There may be certain situations where management will grant a waiver either because compensating controls exist or because the benefits of operating without the control (at least temporarily) outweigh the risk of waiting for full control implementation. Alternatively, there may be times where management implements more stringent controls than generally applied elsewhere. In the example provided the specific control objectives for personnel security and for authentication were assessed. The questionnaire is an excerpt and by no means contains all the questions that would be asked in the area of personnel security and authentication. For brevity, only a few questions were provided in this sample.

An analysis of the levels checked determined that the agency should target improving their background screening implementation and testing. System administrators, programmers, and managers should all have background checks completed prior to accessing the system. The decision to allow access prior to screening was made and checked in the *Risk Based Decision Made* box. Because this box was checked, there should be specific controls implemented to ensure access is not abused, i.e., access is reviewed daily through audit trails, and users have minimal system authority.

Additionally, HGA should improve implementing and testing their password procedures because of the strong need for confidentiality. Without good password management, passwords can be easily guessed and access to the system obtained. The questionnaire's list of objectives is incomplete for both personnel security controls and for authentication controls. Even though the sample is lacking many controls, the completed questionnaire clearly depicts that HGA has policies and procedures in place but there is a strong need for implementing, testing, and reviewing the procedures and controls. The sample indicates that the Training Database would be at level 2.

Category of Sensitivity	Confidentiality	Integrity	Availability
High	X		
Medium			
Low		X	X

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made
Personnel Security						
Are all positions reviewed for sensitivity level?	X	X	X			
Is appropriate background screening for assigned positions completed prior to granting access?	X	X				X
Are there conditions for allowing system access prior to completion of screening?	X	X				
Are sensitive functions divided among different individuals?	X	X	X			
Are mechanisms in place for holding users responsible for their actions?	X	X				
Are termination procedures established?	X	X				
Authentication						
Are passwords, tokens, or biometrics used?	X	X	X			
Do passwords contain alpha numeric, upper/lower case, and special characters?	X	X				
Are passwords changed at least every ninety days or earlier if needed?	X	X				
Is there guidance for handling lost and compromised passwords?	X	X				
Are passwords transmitted and stored with one-way encryption?	X	X				
Is there a limit to the number of invalid access attempts that may occur for a given user?	X	X				

References

Automated Information Systems Security Program Handbook (Release 2.0, May 1994), Department of Health and Human Services, May 1994.

Clinger-Cohen Act of 1996 (formerly known as the Information Management Reform Act), February 10, 1996.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD-99-139, August 1999.

Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

Office of Management and Budget, Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999.

Office of Management and Budget, Memorandum 99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

Office of Management and Budget, Memorandum 00-13, Policies and Data Collection on Federal Web Sites, June 22, 2000.

Paperwork Reduction Act of 1995, 35 U.S. Code 44, January 4, 1995.

Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.

Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Swanson, Marianne and Barbara Guttman, NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP), Gaithersburg, MD, National Institute of Standards and Technology, September 20, 1995.

Swanson, Marianne and Federal Computer Security Program Managers' Forum Working Group, NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, Gaithersburg, MD, National Institute of Standards and Technology, December 1998.

Terminology

Acceptable Risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls.

Accreditation is synonymous with the term **authorize processing**. Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also ***Authorize Processing, Certification,*** and ***Designated Approving Authority.***

Asset is a major application, general support system, high impact program, physical plant, mission critical system, or a logically related group of systems.

Authorize Processing occurs when management authorizes in writing a system based on an assessment of management, operational, and technical controls. By authorizing processing in a system the management official accepts the risks associated with it. See also ***Accreditation, Certification,*** and ***Designated Approving Authority.***

Availability Protection requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

Awareness, Training, and Education includes (1) awareness programs set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in IT security.

Certification is synonymous with the term **authorize processing.** Certification is a major consideration prior to authorizing processing, but not the only consideration. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements. See also ***Accreditation*** and ***Authorize Processing.***

General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Information Owner is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations.

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Material Weakness or ***significant weakness*** is used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.

Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.

Operational Controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Policy a document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance.

Procedures are contained in a document that focuses on the security control areas and management's position.

Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Management is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Rules of Behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of

copyrighted works, unofficial use of Federal government equipment, assignment and limitation of system privileges, and individual accountability.

Sensitive Information refers to information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled.

Sensitivity an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability that is determined by an evaluation of the sensitivity of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

System is a generic term used for briefness to mean either a major application or a general support system.

System Operational Status is either (1) Operational - system is currently in operation, (2) Under Development - system is currently under design, development, or implementation, or (3) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

Technical Controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Threat is an event or activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.

Vulnerability is a flaw or weakness that may allow harm to occur to an IT system or activity.

Appendix D - References

Clinger-Cohen Act of 1996 (formerly known as the Information Management Reform Act), February 10, 1996.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Control Objectives for Information and Related Technology (COBIT) 3rd Edition, Information Systems Audit and Control Foundation, July 2000.

Defense Authorization Act (P.L. 106-398) including Title X, Subtitle G, "Government Information Security Reform," October 28, 2000.

Department of State, Draft Best Security Practices Checklist Appendix A, January 22, 2001.

General Accounting Office, Federal Information System Control Audit Manual (FISCAM), GOA/AIMD-12.19.6, January 1999.

General Accounting Office, Information Security Risk Assessment Practices of Leading Organizations, GAO/AIMD-99-139, August 1999.

ISSO 17799, A Code of Practice for Information Security Management (British Standard 7799),

National Communications System, Public Switched Network Security Assessment Guidelines, September 2000.

Office of Management and Budget, Security of Federal Automated Information Resources, Appendix III to OMB Circular A-130, Management of Federal Information Resources, February 8, 1996.

Office of Management and Budget, Memorandum 99-05, Instructions on Complying with President's Memorandum of May 14, 1998, Privacy and Personal Information in Federal Records, July 1, 1999.

Office of Management and Budget, Memorandum 99-18, Privacy Policies on Federal Web Sites, June 2, 1999.

Office of Management and Budget, Memorandum 00-13, Policies and Data Collection on Federal Web Sites, June 22, 2000.

Paperwork Reduction Act of 1995, 35 U.S. Code 44, January 4, 1995.

Presidential Decision Directive 63, Protecting America's Critical Infrastructures, May 22, 1998.

Presidential Decision Directive 67, Enduring Constitutional Government and Continuity of Government, October 21, 1998.

Stoneburner, Gary, Draft –Rev. A NIST Special Publication 800-30, Risk Management Guide, February 16, 2001.

Swanson, Marianne and Barbara Guttman, NIST Special Publication 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems (GSSP), Gaithersburg, MD, National Institute of Standards and Technology, September 20, 1995.

Swanson, Marianne and Federal Computer Security Program Managers' Forum Working Group, NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, Gaithersburg, MD, National Institute of Standards and Technology, December 1998.

NIST Special Publication 800-53
Revision 2

Recommended Security Controls for Federal Information Systems

Ron Ross
Stu Katzke
Arnold Johnson
Marianne Swanson
Gary Stoneburner
George Rogers

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

December 2007

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James M. Turner, Acting Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-53, Revision 2, 188 pages

(December 2007)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments may be submitted to the Computer Security Division, Information Technology Laboratory, NIST via electronic mail at sec-cert@nist.gov or via regular mail at 100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Compliance with NIST Standards and Guidelines

NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programs to protect their information and information systems.

- Federal Information Processing Standards (FIPS) are developed by NIST in accordance with FISMA. FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.
- Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.[1]
- Other security-related publications, including interagency and internal reports (NISTIRs), and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when so specified by OMB.

Schedule for Compliance with NIST Standards and Guidelines

- For legacy information systems, agencies are expected to be in compliance with NIST security standards and guidelines within one year of the publication date unless otherwise directed by OMB or NIST.[2]
- For information systems under development, agencies are expected to be in compliance with NIST security standards and guidelines immediately upon deployment of the system.

[1] While agencies are required to follow NIST guidance in accordance with OMB policy, there is flexibility within NIST's guidance in how agencies apply the guidance. Unless otherwise specified by OMB, the 800-series guidance documents published by NIST generally allow agencies some latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.

[2] The one-year compliance date for revisions to NIST Special Publications applies only to the new and/or updated material in the publications resulting from the periodic revision process. Agencies are expected to be in compliance with previous versions of NIST Special Publications within one year of the publication date of the previous versions.

Acknowledgments

The authors, Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, and George Rogers, wish to thank their colleagues who reviewed drafts of this document and contributed to its development. A special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support, to Murugiah Souppaya and the NIST information security operations group for their review of the security controls and insightful recommendations, and to Annabelle Lee for her contribution to earlier versions of the document. The authors also gratefully acknowledge and appreciate the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

A special acknowledgment is also given to the participants in the *Industrial Control System (ICS) Security Project* who have put forth significant effort in helping to augment the security controls in NIST Special Publication 800-53 for industrial controls systems. These participants include: Keith Stouffer (NIST), Stu Katzke (NIST), and Marshall Abrams (Mitre Corporation) from the ICS Security Project Development Team; federal agencies participating in the ICS workshops; and individuals and organizations from the public and private sector ICS community providing thoughtful and insightful comments on the proposed augmentations.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

IMPLEMENTING SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory, non-waiverable standard developed in response to the Federal Information Security Management Act of 2002. To comply with the federal standard, agencies must first determine the security category of their information system in accordance with the provisions of FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, and then apply the appropriate set of baseline security controls in NIST Special Publication 800-53 (as amended), *Recommended Security Controls for Federal Information Systems*. Agencies have flexibility in applying the baseline security controls in accordance with the tailoring guidance provided in Special Publication 800-53. This allows agencies to adjust the security controls to more closely fit their mission requirements and operational environments.

The combination of FIPS 200 and NIST Special Publication 800-53 requires a foundational level of security for all federal information and information systems. The agency's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of "security due diligence" for the federal agency and its contractors.

In addition to the security requirements established by FISMA, there may also be specific security requirements in different business areas within agencies that are governed by other laws, Executive Orders, directives, policies, regulations, or associated governing documents, (e.g., the Health Insurance Portability and Accountability Act of 1996, the Federal Financial Management Improvement Act of 1996, or OMB Circular A-127 on Financial Management Systems). These requirements may not be equivalent to the security requirements and implementing security controls required by FISMA or may enhance or further refine the security requirements and security controls. It is important that agency officials (including authorizing officials, chief information officers, senior agency information security officers, information system owners, information system security officers, and acquisition authorities) take steps to ensure that: (i) all appropriate security requirements are addressed in agency acquisitions of information systems and information system services; and (ii) all required security controls are implemented in agency information systems. See http://csrc.nist.gov/sec-cert/ca-compliance.html for additional information on FISMA compliance.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by the Federal Information Security Management Act (FISMA), NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST standards and guidelines are complementary with standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST is working with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. The common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation from the operation and use of information systems. NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST in the FISMA Implementation Project and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27000-series standards.

Table of Contents

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY CONTROLS TO PROTECT INFORMATION SYSTEMS

The selection and employment of appropriate *security controls* for an information system[3] are important tasks that can have major implications on the operations[4] and assets of an organization as well as the welfare of individuals. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems:

- What security controls are needed to adequately protect the information systems that support the operations and assets of the organization in order for that organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective[5] in their application?

The answers to these questions are not given in isolation but rather in the context of an effective *information security program* for the organization that identifies, controls, and mitigates risks to its information and information systems.[6] The security controls defined in Special Publication 800-53 (as amended) and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined and documented information security program. An effective information security program should include:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level and address information security throughout the life cycle of each organizational information system;

[3] An information system is a discrete set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

[4] Organizational operations include mission, functions, image, and reputation.

[5] Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

[6] The E-Government Act (P.L. 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

- Plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;
- Procedures for detecting, reporting, and responding to security incidents; and
- Plans and procedures for continuity of operations for information systems that support the operations and assets of the organization.

It is of paramount importance that responsible officials within the organization understand the risks and other factors that could adversely affect organizational operations, organizational assets, or individuals. Moreover, these officials must understand the current status of their security programs and the security controls planned or in place to protect their information systems in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated mission(s) with what the Office of Management and Budget (OMB) Circular A-130 defines as *adequate security*, or security commensurate with risk, including the magnitude of harm to individuals, the organization, or its assets resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components[7] of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems;
- Providing a recommendation for minimum security controls for information systems categorized in accordance with Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*;

[7] Information system components include, but are not limited to, mainframes, servers, workstations, network components, operating systems, middleware, and applications. Network components can include, for example, such devices as firewalls, sensors (local or remote), switches, guards, routers, gateways, wireless access points, and network appliances. Servers can include, for example, database servers, authentication servers, electronic mail and web servers, proxy servers, domain name servers, and network time servers. Information system components are either purchased commercially off-the-shelf or are custom-developed and can be deployed in land-based, sea-based, airborne, and/or space-based information systems.

- Providing a stable, yet flexible catalog of security controls for information systems to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies; and
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness.

The guidelines provided in this special publication are applicable to all federal information systems[8] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542.[9] The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems. This publication is intended to provide guidance to federal agencies implementing FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.* In addition to the agencies of the federal government, state, local, and tribal governments, and private sector organizations that compose the critical infrastructure of the United States, are encouraged to use these guidelines, as appropriate.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, and authorizing officials); (ii) individuals with information system development responsibilities (e.g., program and project managers, mission/application owners, system designers, system and application programmers); (iii) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system administrators, information system security officers,); and (iv) individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, and certification agents). Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit from the information in this publication.

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS

To create the most technically sound and broadly applicable set of security controls for information systems, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, and intelligence communities as well as controls defined by national and international standards organizations.[10] The objective of NIST Special Publication 800-53 is to provide a set of security

[8] A federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[9] NIST Special Publication 800-59 provides guidance on identifying an information system as a national security system.

[10] Security controls from the audit, defense, healthcare, intelligence, and standards communities are contained in the following publications: (i) Government Accountability Office, *Federal Information System Controls Audit Manual*; (ii) Department of Defense Instruction 8500.2, *Information Assurance Implementation*; (iii) Department of Health and Human Services Centers for Medicare and Medicaid Services, *Core Security Requirements*; (iv) Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*; (v) NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*; and (vi) International Organization for Standardization/International Electrotechnical Commission 17799:2005, *Code of Practice for Information Security Management.*

controls that is sufficiently rich to satisfy the breadth and depth of security requirements[11] levied on information systems and that is consistent with and complementary to other established security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization's confidence that there is ongoing compliance with its stated security requirements.[12]

1.4 ORGANIZATIONAL RESPONSIBILITIES

Organizations[13] should use FIPS 199 to define security categories for their information systems. This publication associates recommended minimum security controls with FIPS 199 low-impact, moderate-impact, and high-impact security categories. For each information system, the recommendation for minimum security controls from Special Publication 800-53 (i.e., the baseline security controls defined in Appendix D, tailored in accordance with the tailoring guidance in Section 3.3) is intended to be used as a starting point for and input to the organization's risk assessment process.[14] The risk assessment results are used to supplement the tailored baseline resulting in a set of agreed-upon controls documented in the security plan for the information system. While the FIPS 199 security categorization associates the operation of the information system with the potential impact on an organization's operations, assets, or individuals, the incorporation of refined threat and vulnerability information during the risk assessment facilitates supplementing the tailored baseline security controls to address organizational needs and tolerance for risk. The final, agreed-upon set of security controls should be documented with appropriate rationale in the security plan for the information system.[15]

The use of security controls from Special Publication 800-53 and the incorporation of tailored baseline controls as a starting point in the control selection process, facilitates a more consistent level of security across federal information systems. It also offers the needed flexibility to

[11] Security requirements are those requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

[12] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006, provides guidance on assessment methods and procedures for security controls defined in this publication. Special Publication 800-53A can also be used to conduct self-assessments of information systems.

[13] An organization typically exercises direct managerial, operational, and/or financial control over its information systems and the security provided to those systems, including the authority and capability to implement the appropriate security controls necessary to protect organizational operations, organizational assets, and individuals.

[14] Risk assessments can be accomplished in a variety of ways depending on the specific needs of the organization. The assessment of risk is a process that should be incorporated into the system development life cycle. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance on the assessment and mitigation of risk as part of an overall risk management process.

[15] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls. The general guidance in Special Publication 800-18 is augmented by Special Publication 800-53 with recommendations for information and rationale to be included in the system security plan.

appropriately modify the controls based on specific organizational policy and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk to the organization's operations, assets, or to individuals.

Building a more secure information system is a multifaceted undertaking that involves the use of: (i) well-defined system-level security requirements and security specifications; (ii) well-designed information technology products; (iii) sound systems/security engineering principles and practices to effectively integrate information technology products into the information system; (iv) appropriate methods for product/system testing and evaluation; and (v) comprehensive system security planning and life cycle management.[16] From a systems engineering viewpoint, security is just one of many required capabilities for an organizational information system—capabilities that must be funded by the organization throughout the life cycle of the system. Realistically assessing the risks to an organization's operations and assets or to individuals by placing the information system into operation or continuing its operation is of utmost importance. Addressing the information system security requirements must be accomplished with full consideration of the risk tolerance of the organization in light of the potential impacts, cost, schedule, and performance issues associated with the acquisition, deployment, and operation of the system.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control selection and specification including: (i) the structural components of security controls and how the controls are organized into families; (ii) minimum (baseline) security controls; (iii) the use of common security controls in support of organization-wide information security programs; (iv) security controls in external environments; (v) assurance in the effectiveness of security controls; and (vi) the commitment to maintain currency of the individual security controls and the control baselines.
- **Chapter Three** describes the process of selecting and specifying security controls for an information system including: (i) defining the organization's overall approach to managing risk; (ii) categorizing the system in accordance with FIPS 199; (iii) selecting and tailoring the initial set of minimum (baseline) security controls; (iv) supplementing the tailored security control baseline, as necessary, based upon risk assessment results; and (v) updating the controls as part of a comprehensive continuous monitoring process.
- **Supporting appendices** provide more detailed security control selection and specification-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) baseline security controls for low-impact, moderate-impact, and high-impact information systems; (v) minimum assurance requirements; (vi) a master catalog of security controls; (vii) mapping tables relating the security controls in this publication to other standards and control sets; (viii) crosswalks of NIST security standards and guidelines with associated security controls; and (ix) guidance on the application of security controls to industrial control systems.

[16] Successful life cycle management depends on having qualified personnel to oversee and manage the information systems within an organization. The skills and knowledge of organizational personnel with information systems (and information security) responsibilities should be carefully evaluated (e.g., through performance, certification, etc.).

CHAPTER TWO

THE FUNDAMENTALS

SECURITY CONTROL STRUCTURE, ORGANIZATION, BASELINES, AND ASSURANCE

This chapter presents the fundamental concepts associated with security control selection and specification including: (i) the structure of security controls and the organization of the controls in the control catalog; (ii) security control baselines; (iii) the identification and use of common security controls; (iv) security controls in external environments; (v) security control assurance; and (vi) future revisions to the security controls, the control catalog, and baseline controls.

2.1 SECURITY CONTROL ORGANIZATION AND STRUCTURE

Security controls in the security control catalog (Appendix F) have a well-defined organization and structure. The security controls are organized into *classes* and *families* for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical) and seventeen security control families.[17] Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each control family. Table 1 summarizes the classes and families in the security control catalog and the associated family identifiers.

TABLE 1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

[17] The seventeen security control families in NIST Special Publication 800-53 are closely aligned with the seventeen security-related areas in FIPS 200 specifying the minimum security requirements for protecting federal information and information systems. Families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning family, is listed as an operational control but also has characteristics that are consistent with security management as well.

To uniquely identify each control, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family. For example, CP-9 is the ninth control in the Contingency Planning family.

The security control structure consists of three key components: (i) a *control* section; (ii) a *supplemental guidance* section; and (iii) a *control enhancements* section.[18] The following example from the Auditing and Accountability family illustrates the structure of a typical security control.

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* operations within the main body of the control. Assignment and selection operations provide an opportunity for an organization to tailor the security controls to support specific mission, business, or operational needs. For example, an organization can specify the specific events to be audited. Once specified, the organization-defined value becomes part of the control, and the organization is assessed against the completed control statement. Some assignment operations may specify minimum or maximum values that constrain the values that may be input by the organization.

[18] A supplemental guidance section is also used for security control enhancements in situations where the guidance is not generally applicable to the entire control but instead focused on the particular control enhancement.

Selection statements also narrow the potential input values by providing a specific list of items from which the organization must choose.

The supplemental guidance section provides additional information related to a specific security control. Organizations are expected to apply the supplemental guidance as appropriate, when defining, developing, and implementing security controls. In certain instances, the supplemental guidance provides more detail concerning the control requirements or important considerations (and the needed flexibility) for implementing security controls in the context of an organization's operational environment, specific mission requirements, or assessment of risk. In addition, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST Special Publications) are listed in the supplemental guidance section, when appropriate, for the particular security control.

The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the basic control. In the example above, if all three control enhancements are selected, the control designation subsequently becomes AU-2 (1) (2) (3). The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements. In the above example, enhancement (3) is used before (1) and (2) since that enhancement is appropriate at a lower level than the other two. This type of situation arises from the decision to enhance control stability in the face of change by not renumbering existing enhancements when new ones are added or when decisions about placement within baselines change.

2.2 SECURITY CONTROL BASELINES

Organizations are required to employ security controls to meet security requirements defined by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., Federal Information Security Management Act, OMB Circular A-130, Appendix III). The challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective in their application, would most cost-effectively comply with the stated security requirements.[19] Selecting the appropriate set of security controls to meet the specific, and sometimes unique, security requirements of an organization is an important task—a task that demonstrates the organization's commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of their information and information systems.

To assist organizations in making the appropriate selection of security controls for their information systems, the concept of *baseline* controls is introduced. Baseline controls are the minimum security controls recommended for an information system based on the system's

[19] An information system may require security controls at different layers within the system. For example, an operating system or network component typically provides an identification and authentication capability. An application may also provide its own identification and authentication capability rendering an additional level of protection for the overall information system. The selection and specification of security controls should consider components at all layers within the information system as part of effective security and privacy architectures.

security categorization in accordance with FIPS 199.[20] The tailored security control baseline (i.e., the appropriate control baseline from Appendix D tailored in accordance with the guidance in Section 3.3) serves as the *starting point* for organizations in determining the appropriate safeguards and countermeasures necessary to protect their information systems. Because the baselines are intended to be broadly applicable starting points, supplements to the tailored baselines (see Section 3.4) will likely be necessary in order to achieve adequate risk mitigation. The tailored baselines are supplemented based on organizational assessments of risk and the resulting controls documented in the security plans for the information systems.

Appendix D provides a listing of baseline security controls. Three sets of baseline controls have been identified corresponding to the low-impact, moderate-impact, and high-impact levels defined in the security categorization process in FIPS 199 and derived in Section 3.2. Each of the three baselines provides an initial set of security controls for a particular impact level associated with a security category.[21] Appendix F provides the complete catalog of security controls for information systems, arranged by control families. The catalog represents the entire set of security controls defined at this time. Chapter 3 provides additional information on how to use security categories to select the appropriate set of baseline security controls, how to apply the tailoring guidance to the baseline controls, and how to supplement the tailored baseline in order to achieve adequate risk mitigation.

Implementation Tip

Since the baseline security controls represent the minimum controls for low-impact, moderate-impact, and high-impact information systems, respectively, there are additional controls and control enhancements that appear in the catalog that are found in only higher-impact baselines or not used in any of the baselines. These additional security controls and control enhancements for the information system are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate. At the end of the security control selection and specification process, the agreed-upon set of security controls documented in the security plan, must be sufficient to provide adequate security for the organization and mitigate risks to its operations, assets, and individuals.

2.3 COMMON SECURITY CONTROLS

An organization-wide view of an information security program facilitates the identification of *common security controls* that can be applied to one or more organizational information systems. Common security controls can apply to: (i) all organizational information systems; (ii) a group of information systems at a specific site; or (iii) common information systems, subsystems, or applications (i.e., common hardware, software, and/or firmware) deployed at multiple operational sites. Common security controls have the following properties:

[20] FIPS 199 security categories are based on the potential impact on an organization or individuals should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

[21] The baseline security controls contained in Appendix D are not necessarily absolutes in that the tailoring guidance described in Section 3.3 provides the organization the ability to eliminate certain controls or specify compensating controls under strict terms and conditions.

- The development, implementation, and assessment of common security controls can be assigned to responsible organizational officials or organizational elements (other than the information system owners whose systems will implement or use the common security controls); and
- The results from the assessment of the common security controls can be used to support the security certification and accreditation processes of organizational information systems where the controls have been applied.[22]

The identification of common security controls is most effectively accomplished as an organization-wide exercise with the involvement of the chief information officer, senior agency information security officer, authorizing officials, information system owners/program managers, information owners, and information system security officers. The organization-wide exercise considers the categories of information systems within the organization in accordance with FIPS 199 (i.e., low-impact, moderate-impact, or high-impact information systems) and the minimum security controls necessary to protect the operations and assets supported by those systems (see *baseline* security controls in Section 2.2). For example, common security controls can be identified for all low-impact information systems by considering the baseline security controls for that category of information system. Similar exercises can be conducted for moderate-impact and high-impact systems as well.

Many of the security controls needed to protect an information system (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) may be excellent candidates for common security control status. By centrally managing the development, implementation, and assessment of the common security controls designated by the organization, security costs can be amortized across multiple information systems. Security controls not designated as common controls are considered *system-specific controls* and are the responsibility of the information system owner. Security plans for individual information systems should clearly identify which security controls have been designated by the organization as common security controls and which controls have been designated as system-specific controls.

Organizations may also assign a *hybrid* status to security controls in situations where one part of the control is deemed to be common, while another part of the control is deemed to be system-specific. For example, an organization may view the IR-1 (Incident Response Policy and Procedures) security control as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid controls may also serve as templates for further control refinement. An organization may choose, for example, to implement the CP-2 (Contingency Planning) security control as a master template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific issues.

Information system owners are responsible for any system-specific issues associated with the implementation of an organization's common security controls. These issues are identified and described in the system security plans for the individual information systems. The senior agency information security officer, acting on behalf of the chief information officer, should coordinate with organizational officials (e.g., facilities managers, site managers, personnel managers) responsible for the development and implementation of the designated common security controls to ensure that the required controls are put into place, the controls are assessed, and the

[22] NIST Special Publication 800-37 provides guidance on security certification and accreditation of information systems.

assessment results are shared with the appropriate information system owners to better support the security accreditation process.

Partitioning security controls into common controls and system-specific controls can result in significant savings to the organization in development and implementation costs especially when the common controls serve multiple information systems and entities. It can also result in a more consistent application of the security controls across the organization at large. Moreover, equally significant savings can be realized in the security certification and accreditation process. Rather than assessing common security controls in every information system, the certification process draws upon any applicable results from the most current assessment of the common security controls performed at the organization level. An organization-wide approach to reuse and sharing of assessment results can greatly enhance the efficiency of the security certifications and accreditations being conducted by organizations and significantly reduce security program costs.

While the concept of security control partitioning into common security controls and system-specific controls is straightforward and intuitive, the application of this principle within an organization takes planning, coordination, and perseverance. If an organization is just beginning to implement this approach or has only partially implemented this approach, it may take some time to get the maximum benefits from security control partitioning and the associated reuse of assessment evidence. Because of the potential dependence on common security controls by many of an organization's information systems, a failure of such common controls may result in a significant increase in agency-level risk—risk that arises from the operation of the systems that depend on these controls.

Implementation Tip

The FIPS 199 security categorization process and the selection of common security controls are closely related activities that are most effectively accomplished on an organization-wide basis with the involvement of the organization's senior leadership (i.e., authorizing officials, chief information officer, senior agency information security officer, information system owners, and mission/information owners). These individuals have the collective corporate knowledge to understand the organization's priorities, the importance of the organization's operations (including mission, functions, image, and reputation) and assets, and the relative importance of the organizational information systems that support those operations and assets. The organization's senior leaders are also in the best position to select the common security controls for each of the security control baselines and assign organizational responsibilities for developing, implementing, and assessing those controls.

2.4 SECURITY CONTROLS IN EXTERNAL ENVIRONMENTS

Organizations are becoming increasingly reliant on information system services provided by external service providers to carry out important missions and functions. External information system services are services that are implemented outside of the system's accreditation boundary (i.e., services that are used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business[23] arrangements), licensing agreements, and/or supply

[23] In March 2004, OMB initiated a governmentwide analysis of selected lines of business supporting the President's Management Agenda goal to expand Electronic Government. Interagency task forces examined business and information technology data and best practices for each line of business—Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure. The goal of the effort is to identify opportunities to reduce the cost of government and improve services to citizens through business performance improvements.

chain exchanges. The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of information system security. These challenges include, but are not limited to: (i) defining the types of external services provided to the organization;[24] (ii) describing how the external services are protected in accordance with the security requirements of the organization; and (iii) obtaining the necessary assurances that the risk to the organization's operations and assets, and to individuals, arising from the use of the external services is at an acceptable level.

The assurance or confidence that the risk to the organization's operations, assets, and individuals is at an acceptable level depends on the trust[25] that the authorizing official places in the external service provider. In some cases, the level of trust is based on the amount of direct control the authorizing official is able to exert on the external service provider with regard to the employment of appropriate security controls necessary for the protection of the service and the evidence brought forth as to the effectiveness of those controls. The level of control is usually established by the terms and conditions of the contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed security control requirements for the provider[26]) to very limited (e.g., using a contract or service-level agreement to obtain commodity services[27] such as commercial telecommunications services). In other cases, the level of trust is derived from other factors that convince the authorizing official that the requisite security controls have been employed and that a credible determination of control effectiveness exists. For example, a separately accredited external information system service provided to a federal agency through a line of business relationship may provide a degree of trust in the external service within the tolerable risk range of the authorizing official.

[24] Information exchanges may be required among the many possible relationships with external service providers. The risk of exchanging information among business partners and other external entities must be assessed and appropriate security controls employed. There may be contract language that establishes specific requirements to protect information exchanged and/or that specifies particular remedies for failure to protect the information as prescribed. In addition, there may be laws or regulations that protect this information from unauthorized disclosure.

[25] The level of trust that an organization places in an external service provider can vary widely ranging from those who are highly trusted (e.g., business partners in a joint venture that share a common business model and common goals) to those who are less trusted and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector).

[26] In reality, the provision of services by providers external to the organization may result in some services without explicit agreements between the organization and the external entities responsible for the services. Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements, etc.), the organization should develop such agreements and require the use of the security controls in Special Publication 800-53. When the organization is not in a position to require explicit agreements with external service providers (e.g., when the service is imposed on the organization or when the service is commodity service), the organization should establish explicit assumptions about the service capabilities with regard to security. Contracts between the organization and external service providers may also require the active participation of the organization. For example, the organization may be required by the contract to install public key encryption-enabled client software recommended by the service provider.

[27] Normally, commercial providers of commodity-type services (e.g., telecommunications services) organize their business models and services around the concept of shared resources and devices for a broad and diverse customer base. Therefore, unless organizations obtain fully dedicated services from commercial service providers (including dedicated devices and management systems), there will likely be a need for greater reliance on compensating security controls to provide the necessary protections for the information system that relies on those external services. The organization's risk assessment and risk mitigation activities should reflect this situation.

Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate *chain of trust* be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The chain of trust can be very complicated due to the number of entities participating in the consumer-provider relationship and the type of relationship between the parties. External service providers may also in turn outsource the services to other external entities, making the chain of trust even more complicated and difficult to manage. Depending on the nature of the service, it may simply be unwise for the organization to wholly trust the provider—not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating controls or accepts the greater degree of risk to its operations and assets, or to individuals.

2.5 SECURITY CONTROL ASSURANCE

Assurance is the grounds for confidence[28] that the security controls implemented within an information system are effective in their application. Assurance can be obtained in a variety of ways including: (i) actions taken by developers and implementers[29] of security controls in the design, development, and implementation techniques and methods; and (ii) actions taken by security control assessors during the testing and evaluation process to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Assurance considerations related to developers and implementers of security controls are addressed in this special publication. Assurance considerations related to assessors of security controls (including certification agents, evaluators, auditors, inspectors general) are addressed in NIST Special Publication 800-53A.

Appendix E describes the minimum assurance requirements for security controls listed in the low, moderate, and high baselines. For security controls in the low baseline, the emphasis is on the control being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner. For security controls in the moderate baseline, the emphasis is on increasing grounds for confidence in control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific capabilities to increase grounds for confidence that the control meets its function or purpose. For security controls in the high baseline, the emphasis is on requiring within the control the capabilities that are needed to support ongoing, consistent operation of the control and to support continuous improvement in the control's effectiveness. There are additional assurance requirements available to developers and

[28] Confidence that the necessary security controls have been effectively implemented in organizational information systems provides a foundation for trust between organizations that depend upon the information processed, stored, or transmitted by those information systems.

[29] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls for an information system. This may include, for example, hardware and software vendors providing the controls, contractors implementing the controls, or organizational personnel such as information system owners, information system security officers, system and network administrators, or other individuals with security responsibility for the information system.

implementers of security controls supplementing the minimum assurance requirements for the moderate and high baselines in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

2.6 REVISIONS AND EXTENSIONS

The set of security controls listed in the control catalog represents the current state-of-the-practice safeguards and countermeasures for information systems. The security controls will be reviewed and revised periodically to reflect: (i) the experience gained from using the controls; (ii) the changing security requirements within organizations; (iii) emerging threats and attack methods; and (iv) the availability of new security technologies.[30] The controls in the control catalog are expected to change over time, as controls are eliminated or revised and new controls are added. The minimum security controls defined in the low, moderate, and high baselines are also expected to change over time as the level of security and due diligence for mitigating risks within organizations increases. In addition to the need for change, the need for stability will be addressed by requiring that proposed additions, deletions, or modifications to the catalog of security controls go through a rigorous public review process to obtain government and private sector feedback and to build consensus for the changes. A stable, yet flexible and technically rigorous set of security controls will be maintained in the control catalog.

[30] Currently, NIST plans to review and revise the security control catalog and security control baselines in Special Publication 800-53 on a biennial basis. The proposed modifications to security controls and security control baselines will be carefully weighed with each revision cycle, considering the desire for stability on one hand, and the need to respond to changing threats and vulnerabilities, new attack methods, new technologies, and the important objective of raising the foundational level of security over time.

CHAPTER THREE

THE PROCESS

SELECTION AND SPECIFICATION OF SECURITY CONTROLS

This chapter describes the process of selecting and specifying security controls for an information system including: (i) defining the organization's overall approach to managing risk; (ii) categorizing the system in accordance with FIPS 199; (iii) selecting and tailoring the initial set of minimum (baseline) security controls;[31] (iv) supplementing the tailored security control baseline as necessary based upon an organizational assessment of risk; and (v) updating the controls as part of a comprehensive continuous monitoring process.

3.1 MANAGING RISK

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program that involves the management of risk—that is, the risk to the organization or to individuals associated with the operation of an information system. The management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, Executive Orders, directives, policies, standards, or regulations. The following activities related to managing risk (also known as the NIST *Risk Management Framework*) are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the system development life cycle and the Federal Enterprise Architecture—

- ***Categorize*** the information system and the information resident within that system based on a FIPS 199 impact analysis.
- ***Select*** an initial set of security controls (i.e., security control baseline from Appendix D) for the information system based on the FIPS 199 security categorization and the minimum security requirements defined in FIPS 200; apply tailoring guidance from Section 3.3 as appropriate, to obtain the control set used as the starting point for the assessment of risk associated with the use of the system.
- ***Supplement*** the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.[32]
- ***Document*** the agreed-upon set of security controls in the system security plan including the organization's rationale for any refinements or adjustments to the initial set of controls.[33]

[31] Tailoring guidance provides organizations with specific considerations on the applicability and implementation of individual security controls in the control baselines (see Section 3.3).

[32] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance on the assessment and mitigation of risk.

[33] NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance on documenting information system security controls.

- ***Implement*** the security controls in the information system. For legacy systems, some or all of the security controls selected may already be in place.
- ***Assess*** the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.[34]
- ***Authorize*** information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable.[35]
- ***Monitor*** and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis.

Figure 1 illustrates the specific activities in the NIST Risk Management Framework and the information security standards and guidance documents associated with each activity.

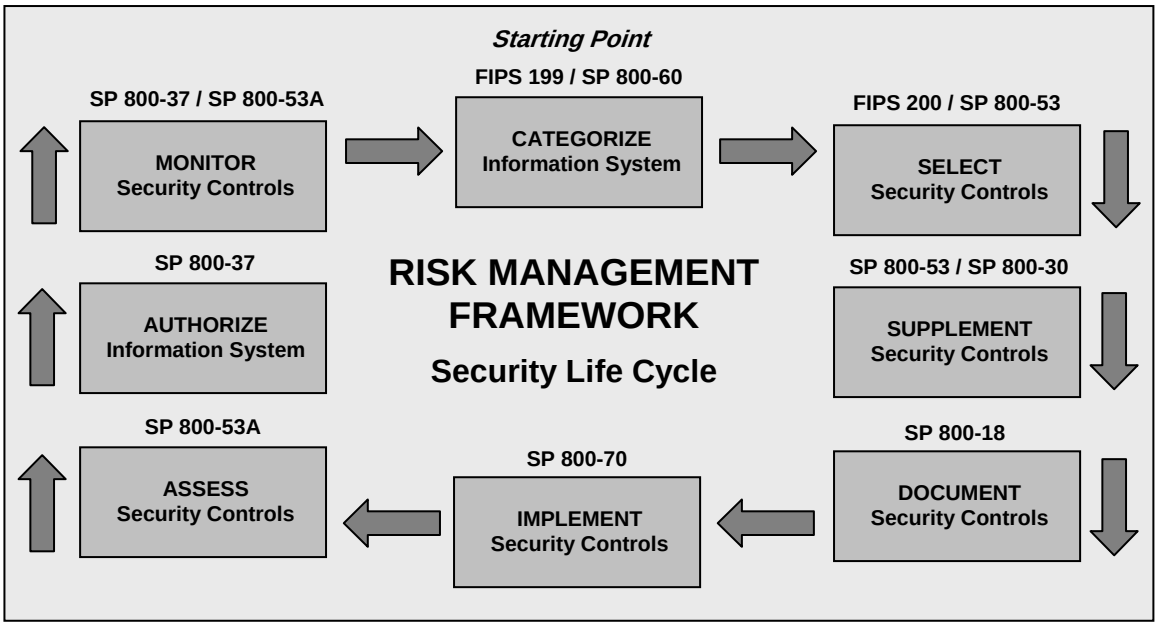


FIGURE 1: THE RISK MANAGEMENT FRAMEWORK

The remainder of this chapter focuses on several key activities in the Risk Management Framework—the FIPS 199 categorization, the initial selection and tailoring of security controls, supplementing the initial controls based on the organization's risk assessment, and updating the controls when necessary.

[34] NIST Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (Second Public Draft), April 2006, provides guidance for determining the effectiveness of security controls.

[35] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidance on the security authorization of information systems.

3.2 SECURITY CATEGORIZATION

FIPS 199, the mandatory federal security categorization standard, is predicated on a simple and well-established concept—determining appropriate priorities for organizational information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system should be commensurate with the potential impact on organizational operations, organizational assets, or individuals should there be a loss of confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information resident on those information systems.[36] The generalized format for expressing the security category (SC) of an information system is:

$$\mathbf{SC}_{\text{information system}} = \{(\textbf{confidentiality}, \textit{impact}), (\textbf{integrity}, \textit{impact}), (\textbf{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is used to determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security control baselines.[37] Thus, a *low-impact* system is defined as an information system in which all three of the security objectives are low. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact* system is an information system in which at least one security objective is high.

Implementation Tip

To determine the overall impact level of the information system:

- First, determine the different types of information that are processed, stored, or transmitted by the information system (e.g., financial sector oversight, inspections and auditing, official information dissemination, etc.). NIST Special Publication 800-60 provides guidance on a variety of information types commonly used by organizations.
- Second, using the impact levels in FIPS 199 and the recommendations of NIST Special Publication 800-60, categorize the confidentiality, integrity, and availability of each information type as low, moderate, or high impact.
- Third, determine the information system security categorization, that is, the highest impact level for each security objective (confidentiality, integrity, availability) from among the categorizations for the information types associated with the information system.
- Fourth, determine the overall impact level of the information system from the highest impact level among the three security objectives in the system security categorization.

[36] NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance on the assignment of security categories to information systems.

[37] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, the security controls in the control catalog are not categorized by security objective—rather, they are grouped into baselines to provide a general protection capability for classes of information systems based on impact level. The application of scoping guidance may allow selective security control baseline tailoring (see Section 3.3).

3.3 SELECTING AND TAILORING THE INITIAL BASELINE

Once the overall impact level of the information system is determined, an initial set of security controls can be selected from the corresponding low, moderate, or high baselines listed in Appendix D. Organizations have the flexibility to tailor the security control baselines in accordance with the terms and conditions set forth in this publication. Tailoring activities include: (i) the application of appropriate *scoping guidance* to the initial baseline; (ii) the specification of *compensating security controls*, if needed; and (iii) the specification of *organization-defined parameters* in the security controls, where allowed. To achieve a cost-effective, risk-based approach to providing adequate information security organization-wide, security control baseline tailoring activities should be coordinated with and approved by appropriate organizational officials (e.g., chief information officers, senior agency information security officers, authorizing officials, or authorizing officials' designated representatives). Tailoring decisions should be documented in the security plan for the information system.[38]

Scoping Guidance

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines. There are several considerations, described below, that can potentially impact how the baseline security controls are applied by the organization:

Common security control-related considerations—

- Security controls designated by the organization as common controls are, in most cases, managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular baseline. Every control in a baseline must be fully addressed either by the organization or the information system owner.

Operational/environmental-related considerations—

- Security controls that are dependent on the nature of the operational environment are applicable only if the information system is employed in an environment necessitating the controls. For example, certain physical security controls may not be applicable to space-based information systems, and temperature and humidity controls may not be applicable to remote sensors that exist outside of the indoor facilities that contain information systems.

Physical Infrastructure-related considerations—

- Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, boundary protection devices, and communications equipment).

[38] It is important for organizations to document the decisions taken during the security control baseline tailoring process, providing a sound rationale for those decisions whenever possible. This documentation is essential when examining the overall security considerations for information systems with respect to potential mission and/or business case impact.

Public access-related considerations—

- Security controls associated with public access information systems should be carefully considered and applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to users accessing information systems through public interfaces. For example, while the baseline controls require identification and authentication of organizational personnel that maintain and support information systems providing the public access services, the same controls might not be required for access to those information systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication would be required for users accessing information systems through public interfaces in some instances, for example, to access/change their personal information.

Technology-related considerations—

- Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system.
- Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control.[39] For example, when information system components are single-user, not networked, or only locally networked, one or more of these characteristics may provide appropriate rationale for not applying selected controls to that component.
- Security controls that can be either explicitly or implicitly supported by automated mechanisms, do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. In situations where automated mechanisms are not readily available, cost-effective, or technically feasible, compensating security controls, implemented through nonautomated mechanisms or procedures, should be used to satisfy specified security controls or control enhancements (see terms and conditions for applying compensating controls below).

Policy/regulatory-related considerations—

- Security controls that address matters governed by applicable laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

[39] For example, auditing controls would typically be applied to the components of an information system that provide or should provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the organization. Organizations should carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an organizational assessment of risk. While the tailoring guidance may support not applying a particular security control to a specific component (e.g., the audit example above), any residual risks associated with the absence of that control must still be addressed and mitigated as necessary to adequately protect the organization's operations, assets, and individuals.

Scalability-related considerations—

- Security controls are scalable with regard to the extent and rigor of the control implementation. Scalability is guided by the FIPS 199 security categorization of the information system being protected. For example, a contingency plan for a FIPS 199 high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for a FIPS 199 low-impact information system may be considerably shorter and contain much less implementation detail. Organizations should use discretion in applying the security controls to information systems, giving consideration to the scalability factors in particular environments. This approach facilitates a cost-effective, risk-based approach to security control implementation that expends no more resources than necessary, yet achieves sufficient risk mitigation and adequate security.

Security objective-related considerations—

- Security controls that uniquely support the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or appropriately modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security categorization for the corresponding security objectives of confidentiality, integrity, or availability before moving to the high water mark;[40] (ii) is supported by an organizational assessment of risk; and (iii) does not affect the security-relevant information within the information system.[41] The following security controls are recommended candidates for downgrading: (i) confidentiality [AC-15, MA-3 (3), MP-2 (1), MP-3, MP-4, MP-5 (1) (2) (3), MP-6, PE-5, SC-4, SC-9]; (ii) integrity [SC-8]; and (iii) availability [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6].[42]

[40] When applying the "high water mark" process in Section 3.2, some of the original FIPS 199 confidentiality, integrity, or availability security objectives may have been upgraded to a higher baseline of security controls. As part of this process, security controls that uniquely support the confidentiality, integrity, or availability security objectives may have been upgraded unnecessarily. Consequently, it is recommended that organizations consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[41] Information that is security-relevant at the system level (e.g., password files, network routing tables, cryptographic key management information) is distinguished from user-level information within an information system. Certain security controls within an information system are used to support the security objectives of confidentiality and integrity for both user-level and system-level information. Caution should be exercised in downgrading confidentiality or integrity-related security controls to ensure that the downgrading action does not result in insufficient protection for the security-relevant information within the information system. Security-relevant information must be protected at the high water mark in order to achieve that level of protection for any of the security objectives related to user-level information.

[42] Certain security controls that are uniquely attributable to confidentiality, integrity, or availability that would ordinarily be considered as potential candidates for downgrading (e.g., AC-16, AU-10, CP-5, IA-7, PE-12, PE-14, PL-5, SC-5, SC-13, SC-14, SC-16) are eliminated from consideration because the controls are either selected for use in all baselines and have no enhancements that could be downgraded, or the controls are optional and not selected for use in any baseline. Organizations should exercise extreme caution when considering downgrading actions on any security controls that do not appear in the list in Section 3.3 to ensure that the downgrading action does not affect security objectives other than the objectives targeted for downgrading.

Compensating Security Controls

With the diverse nature of today's information systems, organizations may find it necessary, on occasion, to specify and employ compensating security controls. A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provides equivalent or comparable protection for an information system.[43] A compensating control for an information system may be employed by an organization only under the following conditions: (i) the organization selects the compensating control from NIST Special Publication 800-53, or if an appropriate compensating control is not available in the security control catalog, the organization adopts a suitable compensating control;[44] (ii) the organization provides a complete and convincing rationale[45] for how the compensating control provides an equivalent security capability or level of protection for the information system and why the related baseline security control could not be employed; and (iii) the organization assesses and formally accepts the risk associated with employing the compensating control in the information system. The use of compensating security controls should be documented in the security plan for the information system and approved by the authorizing official.

Organization-Defined Security Control Parameters

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define selected portions of the controls to support specific organizational requirements or objectives (see AU-2 example in Section 2.1). After the application of the scoping guidance and the selection of compensating security controls, organizations should review the list of security controls for assignment and selection operations and determine appropriate organization-defined values for the identified parameters. Where specified, minimum and maximum values for organization-defined parameters should be adhered to unless more restrictive values are prescribed by applicable laws, Executive Orders, directives, policies, standards, or regulations or are indicated by the risk assessment in order to adequately mitigate risk. Organization-defined security control parameters should be documented in the security plan for the information system.

3.4 SUPPLEMENTING THE TAILORED BASELINE

The tailored security control baseline should be viewed as the foundation or starting point in the selection of adequate security controls for an information system. The tailored baseline represents, for a particular class of information system (derived from the FIPS 199 security categorization and modified appropriately for local conditions), the starting point for determining the needed level of security *due diligence* to be demonstrated by an organization toward the protection of its operations and assets. As described in Section 3.1, the final determination of the appropriate set of security controls necessary to provide adequate security for an information

[43] More than one compensating control may be required to provide the equivalent or comparable protection for a particular security control in NIST Special Publication 800-53. For example, an organization with significant staff limitations may have difficulty in meeting the separation of duty security control but may employ compensating controls by strengthening the audit, accountability, and personnel security controls within the information system.

[44] Organizations should make every attempt to select compensating controls from the security control catalog in NIST Special Publication 800-53. Organization-defined compensating controls should be used only as a last resort when the security control catalog does not contain suitable compensating controls.

[45] The depth and rigor of the rationale provided should be scaled to the FIPS 199 impact level of the information system, with significantly less explanation needed for a low-impact system than for a high-impact system.

system is a function of the organization's assessment of risk and what is required to sufficiently mitigate the risks to organizational operations, organizational assets, or individuals.[46]

In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system or to satisfy the requirements of applicable laws, Executive Orders, directives, policies, standards, or regulations. The risk assessment at this stage in the security control selection process provides important inputs to determine the sufficiency of the security controls in the tailored baseline—that is, the security controls needed to adequately protect the organization's operations (including mission, function, image, and reputation), the organization's assets, and individuals. Organizations are encouraged to make maximum use of the security control catalog to facilitate the process of enhancing security controls or adding controls to the tailored baseline. To assist in this process, the security control catalog in Appendix F contains numerous controls and control enhancements that are found only in higher-impact baselines or are not included in any of the baselines.

There may be situations in which an organization discovers it is employing information technology beyond its ability to adequately protect critical and/or essential missions. That is, the organization cannot apply sufficient security controls within an information system to adequately reduce or mitigate mission risk. In those situations, an alternative strategy is needed to protect the mission from being impeded; a strategy that considers the mission risks that are being brought about by an aggressive use of information technology. Information system use restrictions provide an alternative method to reduce or mitigate risk, for example, when: (i) security controls cannot be implemented within technology and resource constraints; or (ii) security controls lack reasonable expectation of effectiveness against identified threat sources. Restrictions on the use of an information system are sometimes the only prudent or practical course of action to enable mission accomplishment in the face of determined adversaries.

The determination of required system use restrictions should be made by organizational officials having a vested interest in the accomplishment of organizational missions. These officials typically include, but are not limited to, the information system owner, mission owner, authorizing official, senior agency information security officer, and chief information officer. Examples of use restrictions include: (i) limiting either the information an information system can process, store, or transmit or the manner in which a mission is automated; (ii) prohibiting external information system access to critical organizational information by removing selected system components from the network (i.e., air gapping); and (iii) prohibiting moderate- or high-impact information on an information system component to which the public has access, unless an explicit determination is made authorizing such access.

It is important for organizations to document the decisions taken during the security control selection process, providing a sound rationale for those decisions whenever possible. This documentation is essential when examining the overall security considerations for information systems with respect to potential mission and/or business case impact. The resulting set of agreed-upon security controls along with the supporting rationale for control selection decisions and any information system use restrictions are documented in the security plan for the information system.

[46] The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system.

Figure 2 summarizes the security control selection process, including the tailoring of the initial security control baseline and any additional modifications to the baseline required based on the organization's assessment of risk.

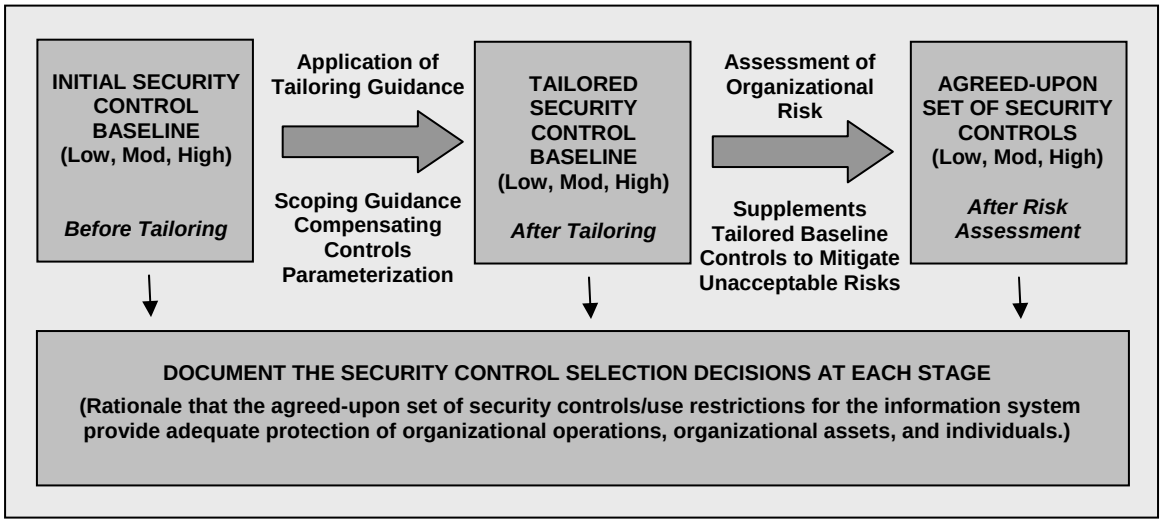


FIGURE 2: SECURITY CONTROL SELECTION PROCESS

3.5 UPDATING SECURITY CONTROLS

As part of a comprehensive continuous monitoring program, organizations should initiate specific actions to determine if there is a need to update the current, agreed-upon set of security controls documented in the security plan and implemented within the information system. Specifically, the organization should revisit, on a regular basis, the risk management activities described in the Risk Management Framework in Section 3.1. Additionally, there are events which can trigger the immediate need to assess the security state of the information system and if required, update the current security controls. These events include, for example:

- An incident results in a breach to the information system, producing a loss of confidence in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;
- A newly identified, credible threat exists to the organization's operations or assets, or to individuals (due to the use of the information system supporting those operations, assets, or individuals) based on law enforcement information, intelligence information, or other credible sources of information; or
- Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment potentially degrade the security state of the system.

When events such as those described above occur, organizations should at a minimum:[47]

[47] Organizations should determine the specific types of events that would trigger a modification to the security plan and changes to the security controls within the information system. The decision to commit resources in light of such events should be guided by an organizational assessment of risk to the organization's operations and assets, or to individuals, that would result if these modifications and changes are not made.

- *Reconfirm the criticality/sensitivity of the information system and the information processed, stored, and/or transmitted by that system.*

  The organization should reexamine the FIPS 199 impact level of the information system to confirm the criticality/sensitivity of the system in supporting its mission operations or business case. The resulting impact on organizational operations, organizational assets, or individuals may provide new insights as to the overall importance of the system in allowing the organization to fulfill its mission responsibilities.

- *Assess the current security state of the information system and reassess the current risk to organizational operations, organizational assets, and individuals.*

  The organization should investigate the information system vulnerability (or vulnerabilities) exploited by the threat source (or that are potentially exploitable by a threat source) and the security controls currently implemented within the system as described in the security plan. The exploitation of an information system vulnerability (or vulnerabilities) by a threat source may be traced to one or more factors including but not limited to: (i) the failure of currently implemented security controls; (ii) missing security controls; (iii) insufficient strength of security controls; and/or (iv) an increase in the sophistication or capability of the threat source. Using the results from the assessment of the current security state, the organization should reassess the risks to organizational operations, organizational assets, or individuals arising from use of the information system.

- *Plan for and initiate any necessary corrective actions.*

  Based on the results of an updated risk assessment, the organization should determine what additional security controls and/or control enhancements may be necessary to address the vulnerability (or vulnerabilities) related to the event or what corrective actions may be needed to fix currently implemented controls deemed to be less than effective.

  The security plan for the information system should then be updated to reflect these corrective actions. A Plan of Action and Milestones (POA&M) should be developed for any deficiencies noted that are not immediately corrected and for the implementation of any security control upgrades or additional controls. After the security controls or control upgrades have been implemented and any other noted deficiencies corrected, the controls should be assessed for effectiveness. The assessment determines if the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the organization's security policy.

- *Consider reaccrediting the information system.*

  Depending on the severity of the event, the impact on organizational operations, organizational assets, or individuals, and the extent of the corrective actions required to fix the identified deficiencies in the information system, the organization may need to consider reaccrediting the information system in accordance with the provisions of NIST Special Publication 800-37. The authorizing official makes the final determination on the need to reaccredit the information system in consultation with the system and mission owners, the senior agency information security officer, and the chief information officer. The authorizing official may choose to conduct an abbreviated reaccreditation focusing only on the affected components of the information system and the associated security controls and/or control enhancements which have been changed during the update. Authorizing officials should have sufficient information from the security certification process to initiate, with an appropriate degree of confidence, the necessary corrective actions to adequately protect individuals and the organization's operations and assets.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.
5. Privacy Act of 1974 (P.L. 93-579), December 1974.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

6. Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106 *Designation of Public Trust Positions and Investigative Requirements*, (5 C.F.R. 731.106).
7. Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305).
8. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
9. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *Business Reference Model* (v2.0), June 2003.
10. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.
11. Director of Central Intelligence Directive 6/3 Policy, *Protecting Sensitive Compartmented Information within Information Systems*, June 1999.
12. Director of Central Intelligence Directive 6/3 Manual, *Protecting Sensitive Compartmented Information within Information Systems*, May 2000.
13. Department of Defense Instruction 8500.2, *Information Assurance Implementation*, February 2003.
14. Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.
15. Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.
16. Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.
17. Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005.

18. Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006.

19. Office of Management and Budget Memorandum M-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2006.

STANDARDS

20. International Organization for Standardization/International Electrotechnical Commission 27001, *Information Security Management System Requirements*, October 2005.

21. International Organization for Standardization/International Electrotechnical Commission 17799, *Code of Practice for Information Security Management*, June 2005.

22. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

    National Institute of Standards and Technology Federal Information Processing Standards Publication 140-3 (Draft), *Security Requirements for Cryptographic Modules*, July 2007.

23. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-2, *Secure Hash Standard (SHS)*, August 2002.

    National Institute of Standards and Technology Federal Information Processing Standards Publication 180-3 (Draft), *Secure Hash Standard (SHS)*, June 2007.

24. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-2, *Digital Signature Standard (DSS)*, January 2000.

    National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3 (Draft), *Digital Signature Standard (DSS)*, March 2006.

25. National Institute of Standards and Technology Federal Information Processing Standards Publication 188, *Standard Security Labels for Information Transfer*, September 1994.

26. National Institute of Standards and Technology Federal Information Processing Standards Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994.

27. National Institute of Standards and Technology Federal Information Processing Standards Publication 197, *Advanced Encryption Standard (AES)*, November 2001.

28. National Institute of Standards and Technology Federal Information Processing Standards Publication 198, *The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

    National Institute of Standards and Technology Federal Information Processing Standards Publication 198-1 (Draft), *The Keyed-Hash Message Authentication Code (HMAC)*, June 2007.

29. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

30. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

31. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, *Personal Identity Verification of Federal Employees and Contractors*, March 2006.

32. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.

33. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.

GUIDELINES

34. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

35. National Institute of Standards and Technology Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995.

36. National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.

37. National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specification for PKI Components (MISPC)*, Version 1, September 1997.

38. National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

39. National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998.

40. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

41. National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, October 1999.

42. National Institute of Standards and Technology Special Publication 800-20 (Revised), *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS)*: *Requirements and Procedures*, April 2000.

43. National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005.

44. National Institute of Standards and Technology Special Publication 800-22 (Revised), *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, May 2001.

45. National Institute of Standards and Technology Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

46. National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000.

47. National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.

48. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.

49. National Institute of Standards and Technology Special Publication 800-28, *Guidelines on Active Content and Mobile Code*, October 2001.

50. National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

51. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

52. National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.

53. National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

54. National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

55. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

56. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003.

57. National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

58. National Institute of Standards and Technology Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.

59. National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.

60. National Institute of Standards and Technology Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004.

61. National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*, November 2007.

62. National Institute of Standards and Technology Special Publication 800-39 (Initial Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, October 2007.

63. National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005.

64. National Institute of Standards and Technology Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, January 2002.

65. National Institute of Standards and Technology Special Publication 800-42, *Guideline on Network Security Testing*, October 2003.

66. National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002.

67. National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

68. National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

69. National Institute of Standards and Technology Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, August 2002.

70. National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

71. National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*, November 2002.

    National Institute of Standards and Technology Special Publication 800-48, Revision 1 (Draft), *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*, August 2007.

72. National Institute of Standards and Technology Special Publication 800-49, *Federal S/MIME V3 Client Profile*, November 2002.

73. National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

74. National Institute of Standards and Technology Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.

75. National Institute of Standards and Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005.

76. National Institute of Standards and Technology Special Publication 800-53A (Final Public Draft), *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, December 2007.

77. National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security*, June 2007.

78. National Institute of Standards and Technology Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003.

    National Institute of Standards and Technology Special Publication 800-55, Revision 1 (Draft), *Performance Measurement Guide for Information Security*, September 2007.

79. National Institute of Standards and Technology Special Publication 800-56A (Revised), *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007.

80. National Institute of Standards and Technology Special Publication 800-57 (Revised), *Recommendation on Key Management, Part I: General*, March 2007.

81. National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.

82. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System,* August 2003.

83. National Institute of Standards and Technology Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, June 2004.

National Institute of Standards and Technology Special Publication 800-60, Revision 1 (Draft), *Guide for Mapping Types of Information and Information Systems to Security Categories*, November 2007.

84. National Institute of Standards and Technology Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004.

National Institute of Standards and Technology Special Publication 800-61, Revision 1 (Draft), *Computer Security Incident Handling Guide,* September 2007.

85. National Institute of Standards and Technology Special Publication 800-63, Version 1.0.2, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Guidelines*, April 2006.

86. National Institute of Standards and Technology Special Publication 800-64, Revision 1, *Security Considerations in the Information System Development Life Cycle,* June 2004.

87. National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

88. National Institute of Standards and Technology Special Publication 800-66, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, March 2005.

89. National Institute of Standards and Technology Special Publication 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004.

90. National Institute of Standards and Technology Special Publication 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005.

91. National Institute of Standards and Technology Special Publication 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006.

92. National Institute of Standards and Technology Special Publication 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers*, May 2005.

93. National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, November 2004.

94. National Institute of Standards and Technology Special Publication 800-73, Revision 1, *Interfaces for Personal Identity Verification*, March 2006.

National Institute of Standards and Technology Special Publication 800-73-2 (Draft), *Interfaces for Personal Identity Verification*, October 2007.

95. National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

96. National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005.

97. National Institute of Standards and Technology Special Publication 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, August 2007.

98. National Institute of Standards and Technology Special Publication 800-79, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations*, July 2005.

99. National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006.

100. National Institute of Standards and Technology Special Publication 800-82 (Second Public Draft), *Guide to Industrial Control Systems (ICS) Security*, September 2007.

101. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

102. National Institute of Standards and Technology Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

103. National Institute of Standards and Technology Special Publication 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)*, April 2006.

104. National Institute of Standards and Technology Special Publication 800-85B, *PIV Data Model Test Guidelines*, July 2006.

105. National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

106. National Institute of Standards and Technology Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, March 2007.

107. National Institute of Standards and Technology Special Publication 800-88, *Guidelines For Media Sanitization*, September 2006.

108. National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications* November 2006.

109. National Institute of Standards and Technology Special Publication 800-90 (Revised), *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, March 2007.

110. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

111. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems*, February 2007.

112. National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services*, August 2007.

113. National Institute of Standards and Technology Special Publication 800-96, *PIV Card / Reader Interoperability Guidelines*, September 2006.

114. National Institute of Standards and Technology Special Publication 800-97, *Establishing Robust Security Networks: A Guide to IEEE 802.11i:*, February 2007.

115. National Institute of Standards and Technology Special Publication 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, April 2007.

116. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

117. National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics*, May 2007.

118. National Institute of Standards and Technology Special Publication 800-103 (Draft), *An Ontology of Identity Credentials, Part I: Background and Formulation*, October 2006.

119. National Institute of Standards and Technology Special Publication 800-104, *A Scheme for PIV Visual Card Topography*, June 2007.

120. National Institute of Standards and Technology Special Publication 800-106 (Draft), *Randomized Hashing Digital Signatures*, July 2007.

121. National Institute of Standards and Technology Special Publication 800-107 (Draft), *Recommendation for Using Approved Hash Algorithms*, July 2007.

122. National Institute of Standards and Technology Special Publication 800-110 (Draft), *Information System Security Reference Data Model*, September 2007.

123. National Institute of Standards and Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, August 2007.

124. National Institute of Standards and Technology Special Publication 800-113 (Draft), *Guide to SSL VPNs*, August 2007.

125. National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

126. National Institute of Standards and Technology Special Publication 800-115 (Draft), *Technical Guide to Information Security Testing*, November 2007.

MISCELLANEOUS PUBLICATIONS

127. Department of Health and Human Services Centers for Medicare and Medicaid Services (CMS), *Core Set of Security Requirements*, February 2004.

128. Government Accountability Office, *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6, January 1999.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Accreditation [FIPS 200, NIST SP 800-37]	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
Accreditation Boundary [NIST SP 800-37]	All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.
Accrediting Authority	See Authorizing Official.
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.
Agency	See Executive Agency.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.
Authorize Processing	See Accreditation.
Authorizing Official [FIPS 200, NIST SP 800-37]	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.

Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).
Boundary Protection Device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels.
Certification [FIPS 200, NIST SP 800-37]	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Certification Agent [NIST SP 800-37]	The individual, group, or organization responsible for conducting a security certification.
Certification Practice Statement	A statement of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in a certificate policy or requirements specified in a contract for services).
Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Commodity Service	An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.
Common Carrier	In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions.
Common Security Control [NIST SP 800-37]	Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSS Inst. 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Countermeasures [CNSS Inst. 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Controlled Area	Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

External Information System (or Component)	An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system).
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
General Support System [OMB Circular A-130, Appendix III]	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Guard (System) [CNSS Inst. 4009, Adapted]	A mechanism limiting the exchange of information between information systems or subsystems.
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Incident [FIPS 200]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.
Information [FIPS 199]	An instance of an information type.

Information Owner [CNSS Inst. 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Policy [CNSS Inst. 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information System [44 U.S.C., Sec. 3502] [OMB Circular A-130, Appendix III]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Owner (or Program Manager) [CNSS Inst. 4009, Adapted]	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Officer [CNSS Inst. 4009, Adapted]	Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.
Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Label	See Security Label.
Line of Business	The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.
Local Access	Access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Major Application [OMB Circular A-130, Appendix III]	An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
Major Information System [OMB Circular A-130]	An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.
Malicious Code [CNSS Inst. 4009] [NIST SP 800-61]	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Malware	See Malicious Code.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Access Control Address	A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.
Media Sanitization [NIST SP 800-88]	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.
Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.
National Security Emergency Preparedness Telecommunications Services [47 C.F.R., Part 64, App A]	Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.
National Security Information	Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Non-repudiation [CNSS Inst. 4009]	Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200]	A federal agency or, as appropriate, any of its operational elements.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Privacy Impact Assessment [OMB Memorandum 03-22]	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged Function	A function executed on an information system involving the control, monitoring, or administration of the system.
Privileged User [CNSS Inst. 4009]	Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, information system security officer, maintainer, system programmer).
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Remote Access	Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Remote Maintenance	Maintenance activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet).
Risk [FIPS 200]	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Risk Assessment [NIST SP 800-30, Adapted]	The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.
Risk Management [FIPS 200]	The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Safeguards [CNSS Inst. 4009, Adapted]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Scoping Guidance	Provides organizations with specific policy/regulatory-related, technology-related, physical infrastructure-related, operational/environmental-related, public access-related, scalability-related, common security control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the control baseline.
Security Category [FIPS 199]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.
Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Baseline [FIPS 200]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Control Enhancements	Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.
Security Functions	The hardware, software, and firmware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis [NIST SP 800-37]	The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.
Security Incident	See Incident.
Security Label	Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Perimeter	See Accreditation Boundary.
Security Plan	See System Security Plan.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See Information System.
System-specific Security Control [NIST SP 800-37]	A security control for an information system that has not been designated as a common security control.

System Security Plan [NIST SP 800-18, Rev 1]	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Tailoring	The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.
Tailored Security Control Baseline	Set of security controls resulting from the application of the tailoring guidance to the security control baseline.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat [CNSS Inst. 4009, Adapted]	Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Threat Assessment [CNSS Inst. 4009]	Formal description and evaluation of threat to an information system.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
User [CNSS Inst. 4009]	Individual or (system) process authorized to access an information system.
Vulnerability [CNSS Inst. 4009, Adapted]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Assessment [CNSS Inst. 4009]	Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CNSS	Committee for National Security Systems
DCID	Director of Central Intelligence Directive
DNS	Domain Name System
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security
NIST	National Institute of Standards and Technology
NSTISSI	National Security Telecommunications and Information System Security Instruction
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POAM	Plan of Action and Milestones
SP	Special Publication
TSP	Telecommunications Service Priority
VPN	Virtual Private Network
VoIP	Voice over Internet Protocol

APPENDIX D

MINIMUM SECURITY CONTROLS – SUMMARY

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

The following table lists the minimum security controls, or security control baselines, for low-impact, moderate-impact, and high-impact information systems. The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines.[48] If a security control is selected for one of the baselines, the family identifier and control number are listed in the appropriate column. If a control is not used in a particular baseline, the entry is marked "not selected." Control enhancements, when used to supplement basic security controls, are indicated by the number of the control enhancement. For example, an "IR-2 (1)" in the high baseline entry for the IR-2 security control indicates that the second control from the Incident Response family has been selected along with control enhancement (1). Some security controls and control enhancements in the security control catalog are not used in any of the baselines but are available for use by organizations if needed; for example, when the results of a risk assessment indicate the need for additional controls or control enhancements in order to adequately mitigate risks to individuals, the organization, or its assets. A complete description of security controls, supplemental guidance for the controls, and control enhancements is provided in Appendix F. A detailed listing of security controls and control enhancements for each control baseline is available at http://csrc.nist.gov/sec-cert.

[48] The hierarchical nature applies to the security requirements of each control (i.e., the base control plus all of its enhancements) at the low-impact, moderate-impact, and high-impact level in that the control requirements at a particular impact level (e.g., AC-18 *Wireless Access Restrictions*—Moderate: AC-18 (1)) meets a stronger set of security requirements for that control than the next lower impact level of the same control (e.g., AC-18 *Wireless Access Restrictions*—Low: AC-18). Since the numerical designation of a control enhancement is neither indicative of the relative strength of the enhancement nor assumes any hierarchical relationship among enhancements, there are some controls (e.g., IA-2) that may not appear to satisfy the hierarchical nature of the security requirements of each control even though they do. For example, with IA-2 *User Identification and Authentication*, enhancement (1) is called out for the moderate baseline and enhancements (2) and (3) are called out for the high baseline. In this case, high [IA-2(2)(3)] is hierarchical to moderate [IA-2(1)] with regard to the security requirements being imposed.

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Control for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	Not Selected	Not Selected	Not Selected
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3)	AU-2 (1) (2) (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	AU-6 (2)	AU-6 (1) (2)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
Certification, Accreditation, and Security Assessments				
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2	CA-2
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4	CA-4 (1)	CA-4 (1)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7
Configuration Management				
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	Not Selected	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1) (2)
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	CP-4	CP-4 (1)	CP-4 (1) (2)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (4)	CP-9 (1) (2) (3) (4)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2	IA-2 (1)	IA-2 (2) (3)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
IA-5	Authenticator Management	IA-5	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
Incident Response				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1)
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
Maintenance				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1) (2) (3)
MA-4	Remote Maintenance	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
Media Protection				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Labeling	Not Selected	Not Selected	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (1) (2)	MP-5 (1) (2) (3)
MP-6	Media Sanitization and Disposal	MP-6	MP-6	MP-6 (1) (2)
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	Not Selected	PE-4
PE-5	Access Control for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10 (1)
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected
Planning				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6
Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	Not Selected	RA-5	RA-5 (1) (2)
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SA-9	External Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11
System and Communications Protection				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information Remnance	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4) (5)	SC-7 (1) (2) (3) (4) (5) (6)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	Not Selected	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring Tools and Techniques	Not Selected	SI-4 (4)	SI-4 (2) (4) (5)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	Not Selected	Not Selected	SI-6

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7 (1) (2)
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12

APPENDIX E

MINIMUM ASSURANCE REQUIREMENTS

LOW, MODERATE, AND HIGH BASELINE APPLICATIONS

The minimum assurance requirements for security controls described in the security control catalog are listed below. The assurance requirements are directed at the activities and actions that security control developers and implementers[49] define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis. The requirements are grouped by security control baseline (i.e., low, moderate, and high) since the requirements apply to each control within the respective baseline. Using a format similar to security controls, assurance requirements are followed by supplemental guidance that provides additional detail and explanation of how the requirements are to be applied. Bolded text indicates requirements that appear for the first time in a particular baseline.

Low Baseline

Assurance Requirement: **The security control is in effect and meets explicitly identified functional requirements in the control statement.**

Supplemental Guidance: For security controls in the low baseline, the focus is on the controls being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

Moderate Baseline

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. **The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.**

Supplemental Guidance: For security controls in the moderate baseline, the focus is on actions supporting increased confidence in the correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation supporting increased confidence that the control meets its required function or purpose. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

High Baseline

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties **and design/implementation** of the control with sufficient detail to permit analysis

[49] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls for an information system. This may include, for example, hardware and software vendors providing the controls, contractors implementing the controls, or organizational personnel such as information system owners, information system security officers, system and network administrators, or other individuals with security responsibility for the information system.

and testing of the control (**including functional interfaces among control components)**. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will **continuously and consistently (i.e., across the information system)** meet its required function or purpose **and support improvement in the effectiveness of the control**. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in the high baseline, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. This documentation is also needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Additional Requirements Enhancing the Moderate and High Baselines

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions supporting increased confidence that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. **The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.**

Supplemental Guidance: The additional high assurance requirements are intended to supplement the minimum assurance requirements for the moderate and high baselines, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-financed threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, SUPPLEMENTAL GUIDANCE, AND CONTROL ENHANCEMENTS

The following catalog of security controls provides a range of safeguards and countermeasures for information systems. The security controls are organized into *families* for ease of use in the control selection and specification process. Each family contains security controls related to the security functionality of the family. A standardized, two-character identifier is assigned to uniquely identify each control family. To uniquely identify each control, a numeric identifier is appended to the family identifier to indicate the number of the control within the control family.

The security control structure consists of three key components: (i) a *control* section; (ii) a *supplemental guidance* section; and (iii) a *control enhancements* section. The control section provides a concise statement of the specific security capability needed to protect a particular aspect of an information system. The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* operations within the control.

The supplemental guidance section provides additional information related to a specific security control. Organizations are expected to apply the supplemental guidance as appropriate, when defining, developing, and implementing security controls. In certain instances, the supplemental guidance provides more detail concerning the control requirements or important considerations (and the needed flexibility) for implementing security controls in the context of an organization's operational environment, specific mission requirements, or assessment of risk. In addition, applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance documents (e.g., OMB Circulars, FIPS, and NIST Special Publications) are listed in the supplemental guidance section, when appropriate, for the particular security control.[50]

The control enhancements section provides statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to a basic control's functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so the enhancements can be easily identified when selected to supplement the basic control. The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among enhancements.

[50] NIST Special Publications listed in the supplemental guidance sections of security controls are assumed to refer to the most recent updates to those publications. For example, a reference to NIST Special Publication 800-18 refers to the Special Publication 800-18, Revision 1, which is the latest version of the security planning guideline.

Cautionary Note

The security controls described in this catalog should be employed in federal information systems in accordance with the risk management guidance provided in Chapter Three. This guidance includes the selection of minimum (baseline) security controls based upon the FIPS 199 security categorization of the information system and the tailoring of the minimum (baseline) security controls by: (i) applying appropriate scoping guidance; (ii) specifying compensating controls, if needed; and (iii) inserting organization-defined security control parameters, where allowed. Since the baseline security controls represent the minimum controls for low-impact, moderate-impact, and high-impact information systems, respectively, there are additional controls and control enhancements that appear in the catalog that are not used in any of the baselines. These additional security controls and control enhancements are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used by organizations to strengthen the level of protection provided in lower-level baselines, if deemed appropriate.

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AC-1	**MOD** AC-1	**HIGH** AC-1

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The organization identifies authorized users of the information system and specifies access rights/privileges. The organization grants access to the information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage. The organization requires proper identification for requests to establish information system accounts and approves all such requests. The organization specifically authorizes and monitors the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts. Account managers are notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured. Account managers are also notified when users' information system usage or need-to-know/need-to-share changes.

Control Enhancements:

(1) The organization employs automated mechanisms to support the management of information system accounts.

(2) The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].

(3) The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].

(4) The organization employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

LOW AC-2	**MOD** AC-2 (1) (2) (3) (4)	**HIGH** AC-2 (1) (2) (3) (4)

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. Related security control: SC-13.

Control Enhancements:

(1) The information system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Enhancement Supplemental Guidance: Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

LOW AC-3	**MOD** AC-3 (1)	**HIGH** AC-3 (1)

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few, of many, generalized examples of possible restrictions that are better expressed as flow control than access control are: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability. Related security control: SC-7.

Control Enhancements:

(1) The information system implements information flow control enforcement using explicit labels on information, source, and destination objects as a basis for flow control decisions.

Enhancement Supplemental Guidance: Information flow control enforcement using explicit labels is used, for example, to control the release of certain types of information.

(2) The information system implements information flow control enforcement using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.

(3) The information system implements information flow control enforcement using dynamic security policy mechanisms as a basis for flow control decisions.

LOW Not Selected	**MOD** AC-4	**HIGH** AC-4

AC-5 SEPARATION OF DUTIES

Control: The information system enforces separation of duties through assigned access authorizations.

Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-5	**HIGH** AC-5

AC-6 LEAST PRIVILEGE

Control: The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Supplemental Guidance: The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-6	**HIGH** AC-6

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*] time period. The information system automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*], *delays next login prompt according to* [*Assignment: organization-defined delay algorithm.*]] when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization.

Control Enhancements:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

LOW AC-7	**MOD** AC-7	**HIGH** AC-7

AC-8 SYSTEM USE NOTIFICATION

Control: The information system displays an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

Supplemental Guidance: Privacy and security policies are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems: (i) the system use information is available and when appropriate, is displayed before granting access; (ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) the notice given to public users of the information system includes a description of the authorized uses of the system.

Control Enhancements: None.

LOW AC-8	**MOD** AC-8	**HIGH** AC-8

AC-9 PREVIOUS LOGON NOTIFICATION

Control: The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for any user to [*Assignment: organization-defined number of sessions*].

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** AC-10

AC-11 SESSION LOCK

Control: The information system prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

Supplemental Guidance: Users can directly initiate session lock mechanisms. A session lock is not a substitute for logging out of the information system. Organization-defined time periods of inactivity comply with federal policy; for example, in accordance with OMB Memorandum 06-16, the organization-defined time period is no greater than thirty minutes for remote access and portable devices.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-11	**HIGH** AC-11

AC-12 SESSION TERMINATION

Control: The information system automatically terminates a remote session after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: A remote session is initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Control Enhancements:

(1) Automatic session termination applies to local and remote sessions.

LOW Not Selected	**MOD** AC-12	**HIGH** AC-12 (1)

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.

Supplemental Guidance: The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities. The extent of the audit record reviews is based on the FIPS 199 impact level of the information system. For example, for low-impact systems, it is not intended that security logs be reviewed frequently for every workstation, but rather at central points such as a web proxy or email servers and when specific circumstances warrant review of other audit records. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the review of user activities.

LOW AC-13	**MOD** AC-13 (1)	**HIGH** AC-13 (1)

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication.

Supplemental Guidance: The organization allows limited user activity without identification and authentication for public websites or other publicly available information systems (e.g., individuals accessing a federal information system at http://www.firstgov.gov). Related security control: IA-2.

Control Enhancements:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

LOW AC-14	**MOD** AC-14 (1)	**HIGH** AC-14 (1)

AC-15 AUTOMATED MARKING

Control: The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

Supplemental Guidance: Automated marking refers to markings employed on external media (e.g., hardcopy documents output from the information system). The markings used in external marking are distinguished from the labels used on internal data structures described in AC-16.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** AC-15

AC-16 AUTOMATED LABELING

Control: The information system appropriately labels information in storage, in process, and in transmission.

Supplemental Guidance: Automated labeling refers to labels employed on internal data structures (e.g., records, files) within the information system. Information labeling is accomplished in accordance with: (i) access control requirements; (ii) special dissemination, handling, or distribution instructions; or (iii) as otherwise required to enforce information system security policy.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-17 REMOTE ACCESS

Control: The organization authorizes, monitors, and controls all methods of remote access to the information system.

Supplemental Guidance: Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology). NIST Special Publication 800-63 provides guidance on remote electronic authentication. If the federal Personal Identity Verification (PIV) credential is used as an identification token where cryptographic token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publications 800-73 and 800-78. NIST Special Publication 800-77 provides guidance on IPsec-based virtual private networks. Related security control: IA-2.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

(3) The organization controls all remote accesses through a limited number of managed access control points.

(4) The organization permits remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

LOW AC-17	**MOD** AC-17 (1) (2) (3) (4)	**HIGH** AC-17 (1) (2) (3) (4)

AC-18 WIRELESS ACCESS RESTRICTIONS

Control: The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system.

Supplemental Guidance: NIST Special Publications 800-48 and 800-97 provide guidance on wireless network security. NIST Special Publication 800-94 provides guidance on wireless intrusion detection and prevention.

Control Enhancements:

(1) The organization uses authentication and encryption to protect wireless access to the information system.

(2) The organization scans for unauthorized wireless access points [*Assignment: organization-defined frequency*] and takes appropriate action if such an access points are discovered.

Enhancement Supplemental Guidance: Organizations conduct a thorough scan for unauthorized wireless access points in facilities containing high-impact information systems. The scan is not limited to only those areas within the facility containing the high-impact information systems.

LOW AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (2)

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES

Control: The organization: (i) establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) authorizes, monitors, and controls device access to organizational information systems.

Supplemental Guidance: Portable and mobile devices (e.g., notebook computers, personal digital assistants, cellular telephones, and other computing and communications devices with network connectivity and the capability of periodically operating in different physical locations) are only allowed access to organizational information systems in accordance with organizational security policies and procedures. Security policies and procedures include device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), configuration management, scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Protecting information residing on portable and mobile devices (e.g., employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered in the media protection family. Related security controls: MP-4, MP-5.

Control Enhancements: None.

LOW Not Selected	**MOD** AC-19	**HIGH** AC-19

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental organizations; and federal information systems that are not owned by, operated by, or under the direct control of the organization.

Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system. This control does not apply to the use of external information systems to access organizational information systems and information that are intended for public access (e.g., individuals accessing federal information through public interfaces to organizational information systems). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system.

Control Enhancements:

(1) The organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations where the organization: (i) can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the organizational entity hosting the external information system.

LOW AC-20	**MOD** AC-20 (1)	**HIGH** AC-20 (1)

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: The security awareness and training policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-16 and 800-50 provide guidance on security awareness and training. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AT-1	**MOD** AT-1	**HIGH** AT-1

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [*Assignment: organization-defined frequency, at least annually*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

LOW AT-2	**MOD** AT-2	**HIGH** AT-2

AT-3 SECURITY TRAINING

Control: The organization identifies personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and provides appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties. The organization's security training program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.

Control Enhancements: None.

LOW AT-3	**MOD** AT-3	**HIGH** AT-3

AT-4 SECURITY TRAINING RECORDS

Control: The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Supplemental Guidance: None.

Control Enhancements: None.

LOW AT-4	**MOD** AT-4	**HIGH** AT-4

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and maintains contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: To facilitate ongoing security education and training for organizational personnel in an environment of rapid technology changes and dynamic threats, the organization establishes and institutionalizes contacts with selected groups and associations within the security community. The groups and associations selected are in keeping with the organization's mission requirements. Information sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: The audit and accountability policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW AU-1	**MOD** AU-1	**HIGH** AU-1

AU-2 AUDITABLE EVENTS

Control: The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*].

Supplemental Guidance: The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Additionally, the security audit function is coordinated with the network health and status monitoring function to enhance the mutual support between the two functions by the selection of information to be recorded by each function. The checklists and configuration guides at http://csrc.nist.gov/pcig/cig.html provide recommended lists of auditable events. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to compile audit records from multiple components throughout the system into a systemwide (logical or physical), time-correlated audit trail.

(2) The information system provides the capability to manage the selection of events to be audited by individual components of the system.

(3) The organization periodically reviews and updates the list of organization-defined auditable events.

LOW AU-2	**MOD** AU-2 (3)	**HIGH** AU-2 (1) (2) (3)

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

Supplemental Guidance: Audit record content includes, for most audit records: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event. NIST Special Publication 800-92 provides guidance on computer security log management.

Control Enhancements:

(1) The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

(2) The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.

LOW AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: The organization provides sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements. Related security controls: AU-2, AU-5, AU-6, AU-7, SI-4.

Control Enhancements: None.

LOW AU-4	**MOD** AU-4	**HIGH** AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system alerts appropriate organizational officials in the event of an audit processing failure and takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related security control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

LOW AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING

Control: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

Supplemental Guidance: Organizations increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

Control Enhancements:

(1) The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

(2) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].

LOW Not Selected	**MOD** AU-6 (2)	**HIGH** AU-6 (1) (2)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: Audit reduction, review, and reporting tools support after-the-fact investigations of security incidents without altering original audit records.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.

LOW Not Selected	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

AU-8 TIME STAMPS

Control: The information system provides time stamps for use in audit record generation.

Supplemental Guidance: Time stamps (including date and time) of audit records are generated using internal system clocks.

Control Enhancements:

(1) The organization synchronizes internal information system clocks [*Assignment: organization-defined frequency*].

LOW AU-8	**MOD** AU-8 (1)	**HIGH** AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

Control Enhancements:

(1) The information system produces audit records on hardware-enforced, write-once media.

LOW AU-9	**MOD** AU-9	**HIGH** AU-9

AU-10 NON-REPUDIATION

Control: The information system provides the capability to determine whether a given individual took a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects against later false claims by an individual of not having taken a specific action. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts, time stamps).

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for [*Assignment: organization-defined time period*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. NIST Special Publication 800-61 provides guidance on computer security incident handling and audit record retention.

Control Enhancements: None.

LOW AU-11	**MOD** AU-11	**HIGH** AU-11

FAMILY: CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS **CLASS:** MANAGEMENT

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

Supplemental Guidance: The security assessment and certification and accreditation policies and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security assessment and certification and accreditation policies can be included as part of the general information security policy for the organization. Security assessment and certification and accreditation procedures can be developed for the security program in general, and for a particular information system, when required. The organization defines what constitutes a significant change to the information system to achieve consistent security reaccreditations. NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS

Control: The organization conducts an assessment of the security controls in the information system [*Assignment: organization-defined frequency, at least annually*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: This control is intended to support the FISMA requirement that the management, operational, and technical controls in each information system contained in the inventory of major information systems be assessed with a frequency depending on risk, but no less than annually. The FISMA requirement for (at least) annual security control assessments should *not* be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security certification and accreditation process. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) security certifications conducted as part of an information system accreditation or reaccreditation process (see CA-4); (ii) continuous monitoring activities (see CA-7); or (iii) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

OMB does not require an annual assessment of *all* security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the three-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-4). NIST Special Publication 800-53A provides guidance on security control assessments to include reuse of existing assessment results. Related security controls: CA-4, CA-6, CA-7, SA-11.

Control Enhancements: None.

LOW CA-2	**MOD** CA-2	**HIGH** CA-2

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

Supplemental Guidance: Since FIPS 199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on connecting information systems. Related security controls: SC-7, SA-9.

Control Enhancements: None.

LOW CA-3	**MOD** CA-3	**HIGH** CA-3

CA-4 SECURITY CERTIFICATION

Control: The organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Supplemental Guidance: A security certification is conducted by the organization in support of the OMB Circular A-130, Appendix III requirement for accrediting the information system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring (see CA-7). The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement (see CA-2). NIST Special Publication 800-53A provides guidance on security control assessments. NIST Special Publication 800-37 provides guidance on security certification and accreditation. Related security controls: CA-2, CA-6, SA-11.

Control Enhancements:

(1) The organization employs an independent certification agent or certification team to conduct an assessment of the security controls in the information system.

Enhancement Supplemental Guidance: An independent certification agent or certification team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain of command associated with the information system or to the determination of security control effectiveness. Independent security certification services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted certification services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the certification agent or certification team conducting the assessment of the security controls in the information system. The authorizing official decides on the required level of certifier independence based on the criticality and sensitivity of the information system and the ultimate risk to organizational operations and organizational assets, and to individuals. The authorizing official determines if the level of certifier independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment of the security controls be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner or authorizing official, independence in the certification process can be achieved by ensuring the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official should consult with the Office of the Inspector General, the senior agency information security officer, and the chief information officer to fully discuss the implications of any decisions on certifier independence in the types of special circumstances described above.

LOW CA-4	**MOD** CA-4 (1)	**HIGH** CA-4 (1)

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization develops and updates [*Assignment: organization-defined frequency*], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

Supplemental Guidance: The plan of action and milestones is a key document in the security accreditation package developed for the authorizing official and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. NIST Special Publication 800-30 provides guidance on risk mitigation.

Control Enhancements: None.

LOW CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY ACCREDITATION

Control: The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization [*Assignment: organization-defined frequency, at least every three years*] or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation.

Supplemental Guidance: OMB Circular A-130, Appendix III, establishes policy for security accreditations of federal information systems. The organization assesses the security controls employed within the information system before and in support of the security accreditation. Security assessments conducted in support of security accreditations are called security certifications. The security accreditation of an information system is not a static process. Through the employment of a comprehensive continuous monitoring process (the fourth and final phase of the certification and accreditation process), the critical information contained in the accreditation package (i.e., the system security plan, the security assessment report, and the plan of action and milestones) is updated on an ongoing basis providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative burden of the three-year reaccreditation process, the authorizing official uses the results of the ongoing continuous monitoring process to the maximum extent possible as the basis for rendering a reaccreditation decision. NIST Special Publication 800-37 provides guidance on the security certification and accreditation of information systems. Related security controls: CA-2, CA-4, CA-7.

Control Enhancements: None.

LOW CA-6	**MOD** CA-6	**HIGH** CA-6

CA-7 CONTINUOUS MONITORING

Control: The organization monitors the security controls in the information system on an ongoing basis.

Supplemental Guidance: Continuous monitoring activities include configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting. The organization assesses all security controls in an information system during the initial security accreditation. Subsequent to the initial accreditation and in accordance with OMB policy, the organization assesses a subset of the controls annually during continuous monitoring. The selection of an appropriate subset of security controls is based on: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; and (iii) the level of assurance (or grounds for confidence) that the organization must have in determining the effectiveness of the security controls in the information system. The organization establishes the selection criteria and subsequently selects a subset of the security controls employed within the information system for assessment. The organization also establishes the schedule for control monitoring to ensure adequate coverage is achieved. Those security controls that are volatile or critical to protecting the information system are assessed at least annually. All other controls are assessed at least once during the information system's three-year accreditation cycle. The organization can use the current year's assessment results obtained during continuous monitoring to meet the annual FISMA assessment requirement (see CA-2).

This control is closely related to and mutually supportive of the activities required in monitoring configuration changes to the information system. An effective continuous monitoring program results in ongoing updates to the information system security plan, the security assessment report, and the plan of action and milestones—the three principle documents in the security accreditation package. A rigorous and well executed continuous monitoring process significantly reduces the level of effort required for the reaccreditation of the information system. NIST Special Publication 800-37 provides guidance on the continuous monitoring process. NIST Special Publication 800-53A provides guidance on the assessment of security controls. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4.

Control Enhancements:

(1) The organization employs an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis.

Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent certification agent or team to assess all of the security controls during the information system's three-year accreditation cycle. Related security controls: CA-2, CA-4, CA-5, CA-6, CM-4.

LOW CA-7	**MOD** CA-7	**HIGH** CA-7

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: The configuration management policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains a current baseline configuration of the information system.

Supplemental Guidance: This control establishes a baseline configuration for the information system. The baseline configuration provides information about a particular component's makeup (e.g., the standard software load for a workstation or notebook computer including updated patch information) and the component's logical placement within the information system architecture. The baseline configuration also provides the organization with a well-defined and documented specification to which the information system is built and deviations, if required, are documented in support of mission needs/objectives. The baseline configuration of the information system is consistent with the Federal Enterprise Architecture. Related security controls: CM-6, CM-8.

Control Enhancements:

(1) The organization updates the baseline configuration of the information system as an integral part of information system component installations.

(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

LOW CM-2	**MOD** CM-2 (1)	**HIGH** CM-2 (1) (2)

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization authorizes, documents, and controls changes to the information system.

Supplemental Guidance: The organization manages configuration changes to the information system using an organizationally approved process (e.g., a chartered Configuration Control Board). Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications. Configuration change control includes changes to the configuration settings for information technology products (e.g., operating systems, firewalls, routers). The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. The approvals to implement a change to the information system include successful results from the security analysis of the change. The organization audits activities associated with configuration changes to the information system. Related security controls: CM-4, CM-6, SI-2.

Control Enhancements:

(1) The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

LOW Not Selected	**MOD** CM-3	**HIGH** CM-3 (1)

CM-4 MONITORING CONFIGURATION CHANGES

Control: The organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes.

Supplemental Guidance: Prior to change implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system. Related security control: CA-7.

Control Enhancements: None.

LOW Not Selected	**MOD** CM-4	**HIGH** CM-4

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes.

Supplemental Guidance: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.

Control Enhancements:

(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

LOW Not Selected	**MOD** CM-5	**HIGH** CM-5 (1)

CM-6 CONFIGURATION SETTINGS

Control: The organization: (i) establishes mandatory configuration settings for information technology products employed within the information system; (ii) configures the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) documents the configuration settings; and (iv) enforces the configuration settings in all components of the information system.

Supplemental Guidance: Configuration settings are the configurable parameters of the information technology products that compose the information system. Organizations monitor and control changes to the configuration settings in accordance with organizational policies and procedures. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on producing and using configuration settings for information technology products employed in organizational information systems. Related security controls: CM-2, CM-3, SI-4.

Control Enhancements:

(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

LOW CM-6	**MOD** CM-6	**HIGH** CM-6 (1)

CM-7 LEAST FUNCTIONALITY

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, the organization limits component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, File Transfer Protocol, Hyper Text Transfer Protocol, file sharing).

Control Enhancements:

(1) The organization reviews the information system [*Assignment: organization-defined frequency*], to identify and eliminate unnecessary functions, ports, protocols, and/or services.

LOW Not Selected	**MOD** CM-7	**HIGH** CM-7 (1)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization develops, documents, and maintains a current inventory of the components of the information system and relevant ownership information.

Supplemental Guidance: The organization determines the appropriate level of granularity for the information system components included in the inventory that are subject to management control (i.e., tracking, and reporting). The inventory of information system components includes any information determined to be necessary by the organization to achieve effective property accountability (e.g., manufacturer, model number, serial number, software license information, system/component owner). The component inventory is consistent with the accreditation boundary of the information system. Related security controls: CM-2, CM-6.

Control Enhancements:

(1) The organization updates the inventory of information system components as an integral part of component installations.

(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

LOW CM-8	**MOD** CM-8 (1)	**HIGH** CM-8 (1) (2)

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: The contingency planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-34 provides guidance on contingency planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW CP-1	**MOD** CP-1	**HIGH** CP-1

CP-2 CONTINGENCY PLAN

Control: The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during crisis situations.

LOW CP-2	**MOD** CP-2 (1)	**HIGH** CP-2 (1) (2)

CP-3 CONTINGENCY TRAINING

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

LOW Not Selected	**MOD** CP-3	**HIGH** CP-3 (1)

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization: (i) tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) reviews the contingency plan test/exercise results and initiates corrective actions.

Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., full-scale contingency plan testing, functional/tabletop exercises). The depth and rigor of contingency plan testing and/or exercises increases with the FIPS 199 impact level of the information system. Contingency plan testing and/or exercises also include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan. NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Control Enhancements:

(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan.

(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

(3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.

LOW CP-4	**MOD** CP-4 (1)	**HIGH** CP-4 (1) (2)

CP-5 CONTINGENCY PLAN UPDATE

Control: The organization reviews the contingency plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

Supplemental Guidance: Organizational changes include changes in mission, functions, or business processes supported by the information system. The organization communicates changes to appropriate organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan).

Control Enhancements: None.

LOW CP-5	**MOD** CP-5	**HIGH** CP-5

CP-6 ALTERNATE STORAGE SITE

Control: The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives.

Control Enhancements:

(1) The organization identifies an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.

(2) The organization configures the alternate storage site to facilitate timely and effective recovery operations.

(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

LOW Not Selected	**MOD** CP-6 (1) (3)	**HIGH** CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITE

Control: The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary processing capabilities are unavailable.

Supplemental Guidance: Equipment and supplies required to resume operations within the organization-defined time period are either available at the alternate site or contracts are in place to support delivery to the site. Timeframes to resume information system operations are consistent with organization-established recovery time objectives.

Control Enhancements:

(1) The organization identifies an alternate processing site that is geographically separated from the primary processing site so as not to be susceptible to the same hazards.

(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(4) The organization fully configures the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability.

LOW Not Selected	**MOD** CP-7 (1) (2) (3)	**HIGH** CP-7 (1) (2) (3) (4)

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: In the event that the primary and/or alternate telecommunications services are provided by a common carrier, the organization requests Telecommunications Service Priority (TSP) for all telecommunications services used for national security emergency preparedness (see http://tsp.ncs.gov for a full explanation of the TSP program).

Control Enhancements:

(1) The organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(2) The organization obtains alternate telecommunications services that do not share a single point of failure with primary telecommunications services.

(3) The organization obtains alternate telecommunications service providers that are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.

(4) The organization requires primary and alternate telecommunications service providers to have adequate contingency plans.

LOW Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [*Assignment: organization-defined frequency*] and protects backup information at the storage location.

Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control. Related security controls: MP-4, MP-5.

Control Enhancements:

(1) The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.

(2) The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.

(3) The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.

(4) The organization protects system backup information from unauthorized modification.

Enhancement Supplemental Guidance: The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control. Related security controls: MP-4, MP-5.

LOW CP-9	**MOD** CP-9 (1) (4)	**HIGH** CP-9 (1) (2) (3) (4)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

Supplemental Guidance: Information system recovery and reconstitution to a known secure state means that all system parameters (either default or organization-established) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded, and the system is fully tested.

Control Enhancements:

(1) The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.

LOW CP-10	**MOD** CP-10	**HIGH** CP-10 (1)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: The identification and authentication policy and procedures are consistent with: (i) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (ii) other applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW IA-1	**MOD** IA-1	**HIGH** IA-1

IA-2 USER IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

Supplemental Guidance: Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance security control AC-14. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. NIST Special Publication 800-63 provides guidance on remote electronic authentication including strength of authentication mechanisms. For purposes of this control, the guidance provided in Special Publication 800-63 is applied to both local and remote access to information systems. Remote access is any access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet). Local access is any access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network. Unless a more stringent control enhancement is specified, authentication for both local and remote information system access is NIST Special Publication 800-63 level 1 compliant. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. In addition to identifying and authenticating users at the information system level (i.e., at system logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization.

In accordance with OMB policy and E-Authentication E-Government initiative, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. The e-authentication risk assessment conducted in accordance with OMB Memorandum 04-04 is used in determining the NIST Special Publication 800-63 compliance requirements for such accesses with regard to the IA-2 control and its enhancements. Scalability, practicality, and security issues are simultaneously considered in balancing the need to ensure ease of use for public access to such information and information systems with the need to protect organizational operations, organizational assets, and individuals. Related security controls: AC-14, AC-17.

Control Enhancements:

(1) The information system employs multifactor authentication for *remote* system access that is NIST Special Publication 800-63 [*Selection: organization-defined level 3, level 3 using a hardware authentication device, or level 4*] compliant.

(2) The information system employs multifactor authentication for *local* system access that is NIST Special Publication 800-63 [*Selection: organization-defined level 3 or level 4*] compliant.

(3) The information system employs multifactor authentication for *remote* system access that is NIST Special Publication 800-63 level 4 compliant.

LOW IA-2	**MOD** IA-2 (1)	**HIGH** IA-2 (2) (3)

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system identifies and authenticates specific devices before establishing a connection.

Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Control Enhancements: None.

LOW Not Selected	**MOD** IA-3	**HIGH** IA-3

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [*Assignment: organization-defined time period*] of inactivity; and (vi) archiving user identifiers.

Supplemental Guidance: Identifier management is not applicable to shared information system accounts (e.g., guest and anonymous accounts). FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors.

Control Enhancements: None.

LOW IA-4	**MOD** IA-4	**HIGH** IA-4

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically.

Supplemental Guidance: Information system authenticators include, for example, tokens, PKI certificates, biometrics, passwords, and key cards. Users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. For password-based authentication, the information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations. For PKI-based authentication, the information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account. In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems (and associated authenticator management) may also be required to protect nonpublic or privacy-related information. FIPS 201 and Special Publications 800-73, 800-76, and 800-78 specify a personal identity verification (PIV) credential for use in the unique identification and authentication of federal employees and contractors. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW IA-5	**MOD** IA-5	**HIGH** IA-5

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password is an example of obscuring feedback of authentication information.

Control Enhancements: None.

LOW IA-6	**MOD** IA-6	**HIGH** IA-6

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system employs authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Supplemental Guidance: The applicable federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect, and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Control Enhancements: None.

LOW IA-7	**MOD** IA-7	**HIGH** IA-7

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Supplemental Guidance: The incident response policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures. NIST Special Publication 800-61 provides guidance on incident handling and reporting. NIST Special Publication 800-83 provides guidance on malware incident handling and prevention.

Control Enhancements: None.

LOW IR-1	**MOD** IR-1	**HIGH** IR-1

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

LOW Not Selected	**MOD** IR-2	**HIGH** IR-2 (1)

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Control: The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency, at least annually*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.

Supplemental Guidance: NIST Special Publication 800-84 provides guidance on test, training, and exercise programs for information technology plans and capabilities.

Control Enhancements:

(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability.

LOW Not Selected	**MOD** IR-3	**HIGH** IR-3 (1)

IR-4 INCIDENT HANDLING

Control: The organization implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The organization incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements the procedures accordingly. Related security controls: AU-6, PE-6.

Control Enhancements:

(1) The organization employs automated mechanisms to support the incident handling process.

LOW IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1)

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents on an ongoing basis.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

LOW Not Selected	**MOD** IR-5	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Control: The organization promptly reports incident information to appropriate authorities.

Supplemental Guidance: The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting authorities or organizations are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Organizational officials report cyber security incidents to the United States Computer Emergency Readiness Team (US-CERT) at http://www.us-cert.gov within the specified timeframe designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. In addition to incident information, weaknesses and vulnerabilities in the information system are reported to appropriate organizational officials in a timely manner to prevent security incidents. NIST Special Publication 800-61 provides guidance on incident reporting.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

LOW IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization's incident response capability.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required.

Control Enhancements:

(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.

LOW IR-7	**MOD** IR-7 (1)	**HIGH** IR-7 (1)

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: The information system maintenance policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW MA-1	**MOD** MA-1	**HIGH** MA-1

MA-2 CONTROLLED MAINTENANCE

Control: The organization schedules, performs, documents, and reviews records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

Supplemental Guidance: All maintenance activities to include routine, scheduled maintenance and repairs are controlled; whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Organizational officials approve the removal of the information system or information system components from the facility when repairs are necessary. If the information system or component of the system requires off-site repair, the organization removes all information from associated media using approved procedures. After maintenance is performed on the information system, the organization checks all potentially impacted security controls to verify that the controls are still functioning properly.

Control Enhancements:

(1) The organization maintains maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).

(2) The organization employs automated mechanisms to schedule and conduct maintenance as required, and to create up-to date, accurate, complete, and available records of all maintenance actions, both needed and completed.

LOW MA-2	**MOD** MA-2 (1)	**HIGH** MA-2 (1) (2)

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.

Supplemental Guidance: The intent of this control is to address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing "ping," "ls," "ipconfig," or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

Control Enhancements:

(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

(3) The organization checks all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.

(4) The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

LOW Not Selected	**MOD** MA-3	**HIGH** MA-3 (1) (2) (3)

MA-4 REMOTE MAINTENANCE

Control: The organization authorizes, monitors, and controls any remotely executed maintenance and diagnostic activities, if employed.

Supplemental Guidance: Remote maintenance and diagnostic activities are conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet). The use of remote maintenance and diagnostic tools is consistent with organizational policy and documented in the security plan for the information system. The organization maintains records for all remote maintenance and diagnostic activities. Other techniques and/or controls to consider for improving the security of remote maintenance include: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques, such as Level 3 or 4 tokens as described in NIST Special Publication 800-63; and (iii) remote disconnect verification. When remote maintenance is completed, the organization (or information system in certain cases) terminates all sessions and remote connections invoked in the performance of that activity. If password-based authentication is used to accomplish remote maintenance, the organization changes the passwords following each remote maintenance service. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency provides a listing of approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm. Related security controls: IA-2, MP-6.

Control Enhancements:

(1) The organization audits all remote maintenance and diagnostic sessions and appropriate organizational personnel review the maintenance records of the remote sessions.

(2) The organization addresses the installation and use of remote maintenance and diagnostic links in the security plan for the information system.

(3) The organization does not allow remote maintenance or diagnostic services to be performed by a provider that does not implement for its own information system, a level of security at least as high as that implemented on the system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system.

LOW MA-4	**MOD** MA-4 (1) (2)	**HIGH** MA-4 (1) (2) (3)

MA-5 MAINTENANCE PERSONNEL

Control: The organization allows only authorized personnel to perform maintenance on the information system.

Supplemental Guidance: Maintenance personnel (whether performing maintenance locally or remotely) have appropriate access authorizations to the information system when maintenance activities allow access to organizational information or could result in a future compromise of confidentiality, integrity, or availability. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the information system.

Control Enhancements: None.

LOW MA-5	**MOD** MA-5	**HIGH** MA-5

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and spare parts for [*Assignment: organization-defined list of key information system components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** MA-6	**HIGH** MA-6

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: The media protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW MP-1	**MOD** MP-1	**HIGH** MP-1

MP-2 MEDIA ACCESS

Control: The organization restricts access to information system media to authorized individuals.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones).

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection.

Control Enhancements:

(1) The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

Enhancement Supplemental Guidance: This control enhancement is primarily applicable to designated media storage areas within an organization where a significant volume of media is stored and is not intended to apply to every location where some media is stored (e.g., in individual offices).

LOW MP-2	**MOD** MP-2 (1)	**HIGH** MP-2 (1)

MP-3 MEDIA LABELING

Control: The organization: (i) affixes external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) exempts [*Assignment: organization-defined list of media types or hardware components*] from labeling so long as they remain within [*Assignment: organization-defined protected environment*].

Supplemental Guidance: An organizational assessment of risk guides the selection of media requiring labeling. Organizations document in policy and procedures, the media requiring labeling and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, labeling is not required for media containing information determined by the organization to be in the public domain or to be publicly releasable.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** MP-3

MP-4 MEDIA STORAGE

Control: The organization physically controls and securely stores information system media within controlled areas.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Organizations document in policy and procedures, the media requiring physical protection and the specific measures taken to afford such protection. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. For example, fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection. The organization protects information system media identified by the organization until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

As part of a defense-in-depth protection strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. FIPS 199 security categorization guides the selection of appropriate candidates for secondary storage encryption. The organization implements effective cryptographic key management in support of secondary storage encryption and provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Related security controls: CP-9, RA-2.

Control Enhancements: None.

LOW Not Selected	**MOD** MP-4	**HIGH** MP-4

MP-5 MEDIA TRANSPORT

Control: The organization protects and controls information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. This control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel exercise extreme caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. An organizational assessment of risk guides the selection of media and associated information contained on that media requiring protection during transport. Organizations document in policy and procedures, the media requiring protection during transport and the specific measures taken to protect such transported media. The rigor with which this control is applied is commensurate with the FIPS 199 security categorization of the information contained on the media. An organizational assessment of risk also guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service).

Control Enhancements:

(1) The organization protects digital and non-digital media during transport outside of controlled areas using [*Assignment: organization-defined security measures, e.g., locked container, cryptography*].

Enhancement Supplemental Guidance: Physical and technical security measures for the protection of digital and non-digital media are approved by the organization, commensurate with the FIPS 199 security categorization of the information residing on the media, and consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used.

(2) The organization documents, where appropriate, activities associated with the transport of information system media using [*Assignment: organization-defined system of records*].

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

(3) The organization employs an identified custodian at all times to transport information system media.

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk.

LOW Not Selected	**MOD** MP-5 (1) (2)	**HIGH** MP-5 (1) (2) (3)

MP-6 MEDIA SANITIZATION AND DISPOSAL

Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal or release for reuse.

Supplemental Guidance: Sanitization is the process used to remove information from information system media such that there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or disposed. The organization uses its discretion on sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposed. NIST Special Publication 800-88 provides guidance on media sanitization. The National Security Agency also provides media sanitization guidance and maintains a listing of approved sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

Control Enhancements:

(1) The organization tracks, documents, and verifies media sanitization and disposal actions.

(2) The organization periodically tests sanitization equipment and procedures to verify correct performance.

LOW MP-6	**MOD** MP-6	**HIGH** MP-6 (1) (2)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: The physical and environmental protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. Designated officials within the organization review and approve the access list and authorization credentials [*Assignment: organization-defined frequency, at least annually*].

Supplemental Guidance: Appropriate authorization credentials include, for example, badges, identification cards, and smart cards. The organization promptly removes from the access list personnel no longer requiring access to the facility where the information system resides.

Control Enhancements: None.

LOW PE-2	**MOD** PE-2	**HIGH** PE-2

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization controls all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facility. The organization controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

Supplemental Guidance: The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (i) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled. Where federal Personal Identity Verification (PIV) credential is used as an identification token and token-based access control is employed, the access control system conforms to the requirements of FIPS 201 and NIST Special Publication 800-73. If the token-based access control function employs cryptographic verification, the access control system conforms to the requirements of NIST Special Publication 800-78. If the token-based access control function employs biometric verification, the access control system conforms to the requirements of NIST Special Publication 800-76.

Control Enhancements:

(1) The organization controls physical access to the information system independent of the physical access controls for the facility.

Enhancement Supplemental Guidance: This control enhancement, in general, applies to server rooms, communications centers, or any other areas within a facility containing large concentrations of information system components or components with a higher impact level than that of the majority of the facility. The intent is to provide an additional layer of physical security for those areas where the organization may be more vulnerable due to the concentration of information system components or the impact level of the components. The control enhancement is not intended to apply to workstations or peripheral devices that are typically dispersed throughout the facility and used routinely by organizational personnel.

LOW PE-3	**MOD** PE-3	**HIGH** PE-3 (1)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** PE-4

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM

Control: The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** PE-5	**HIGH** PE-5

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization monitors physical access to the information system to detect and respond to physical security incidents.

Supplemental Guidance: The organization reviews physical access logs periodically and investigates apparent security violations or suspicious physical access activities. Response to detected physical security incidents is part of the organization's incident response capability.

Control Enhancements:

(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to recognize potential intrusions and initiate appropriate response actions.

LOW PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1) (2)

PE-7 VISITOR CONTROL

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Supplemental Guidance: Government contractors and others with permanent authorization credentials are not considered visitors. Personal Identity Verification (PIV) credentials for federal employees and contractors conform to FIPS 201, and the issuing organizations for the PIV credentials are accredited in accordance with the provisions of NIST Special Publication 800-79.

Control Enhancements:

(1) The organization escorts visitors and monitors visitor activity, when required.

LOW PE-7	**MOD** PE-7 (1)	**HIGH** PE-7 (1)

PE-8 ACCESS RECORDS

Control: The organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization review the visitor access records [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.

(2) The organization maintains a record of all physical access, both visitor and authorized individuals.

LOW PE-8	**MOD** PE-8	**HIGH** PE-8 (1) (2)

PE-9 POWER EQUIPMENT AND POWER CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths.

LOW Not Selected	**MOD** PE-9	**HIGH** PE-9

PE-10 EMERGENCY SHUTOFF

Control: The organization provides, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

Supplemental Guidance: Facilities containing concentrations of information system resources may include, for example, data centers, server rooms, and mainframe rooms.

Control Enhancements:

(1) The organization protects the emergency power-off capability from accidental or unauthorized activation.

LOW Not Selected	**MOD** PE-10	**HIGH** PE-10 (1)

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

LOW Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

Supplemental Guidance: None.

Control Enhancements: None.

LOW PE-12	**MOD** PE-12	**HIGH** PE-12

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire.

Supplemental Guidance: Fire suppression and detection devices/systems include, but are not limited to, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

Control Enhancements:

(1) The organization employs fire detection devices/systems that activate automatically and notify the organization and emergency responders in the event of a fire.

(2) The organization employs fire suppression devices/systems that provide automatic notification of any activation to the organization and emergency responders.

(3) The organization employs an automatic fire suppression capability in facilities that are not staffed on a continuous basis.

LOW PE-13	**MOD** PE-13 (1) (2) (3)	**HIGH** PE-13 (1) (2) (3)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization regularly maintains, within acceptable levels, and monitors the temperature and humidity within the facility where the information system resides.

Supplemental Guidance: None.

Control Enhancements: None.

LOW PE-14	**MOD** PE-14	**HIGH** PE-14

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a significant water leak.

LOW PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes and controls information system-related items entering and exiting the facility and maintains appropriate records of those items.

Supplemental Guidance: The organization controls delivery areas and, if possible, isolates the areas from the information system and media libraries to avoid unauthorized physical access.

Control Enhancements: None.

LOW PE-16	**MOD** PE-16	**HIGH** PE-16

PE-17 ALTERNATE WORK SITE

Control: The organization employs appropriate management, operational, and technical information system security controls at alternate work sites.

Supplemental Guidance: The organization provides a means for employees to communicate with information system security staff in case of security problems. NIST Special Publication 800-46 provides guidance on security in telecommuting and broadband communications.

Control Enhancements: None.

LOW Not Selected	**MOD** PE-17	**HIGH** PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards.

Control Enhancements:

(1) The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.

LOW Not Selected	**MOD** PE-18	**HIGH** PE-18 (1)

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: The FIPS 199 security categorization (for confidentiality) of the information system and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PLANNING **CLASS:** MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: The security planning policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-18 provides guidance on security planning. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 SYSTEM SECURITY PLAN

Control: The organization develops and implements a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization review and approve the plan.

Supplemental Guidance: The security plan is aligned with the organization's information system architecture and information security architecture. NIST Special Publication 800-18 provides guidance on security planning.

Control Enhancements: None.

LOW PL-2	**MOD** PL-2	**HIGH** PL-2

PL-3 SYSTEM SECURITY PLAN UPDATE

Control: The organization reviews the security plan for the information system [*Assignment: organization-defined frequency, at least annually*] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

Supplemental Guidance: Significant changes are defined in advance by the organization and identified in the configuration management process. NIST Special Publication 800-18 provides guidance on security plan updates.

Control Enhancements: None.

LOW PL-3	**MOD** PL-3	**HIGH** PL-3

PL-4 RULES OF BEHAVIOR

Control: The organization establishes and makes readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

Supplemental Guidance: Electronic signatures are acceptable for use in acknowledging rules of behavior unless specifically prohibited by organizational policy. NIST Special Publication 800-18 provides guidance on preparing rules of behavior.

Control Enhancements: None.

LOW PL-4	**MOD** PL-4	**HIGH** PL-4

PL-5 PRIVACY IMPACT ASSESSMENT

Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

Supplemental Guidance: OMB Memorandum 03-22 provides guidance for implementing the privacy provisions of the E-Government Act of 2002.

Control Enhancements: None.

LOW PL-5	**MOD** PL-5	**HIGH** PL-5

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Supplemental Guidance: Routine security-related activities include, but are not limited to, security assessments, audits, system hardware and software maintenance, security certifications, and testing/exercises. Organizational advance planning and coordination includes both emergency and non-emergency (i.e., routine) situations.

Control Enhancements: None.

LOW Not Selected	**MOD** PL-6	**HIGH** PL-6

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: The personnel security policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION CATEGORIZATION

Control: The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [*Assignment: organization-defined frequency*].

Supplemental Guidance: Position risk designations are consistent with 5 CFR 731.106(a) and Office of Personnel Management policy and guidance.

Control Enhancements: None.

LOW PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

Control: The organization screens individuals requiring access to organizational information and information systems before authorizing access.

Supplemental Guidance: Screening is consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; (iii) organizational policy, regulations, and guidance; (iv) FIPS 201 and Special Publications 800-73, 800-76, and 800-78; and (v) the criteria established for the risk designation of the assigned position.

Control Enhancements: None.

LOW PS-3	**MOD** PS-3	**HIGH** PS-3

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment, terminates information system access, conducts exit interviews, retrieves all organizational information system-related property, and provides appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

Supplemental Guidance: Information system-related property includes, for example, keys, identification cards, and building passes. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

LOW PS-4	**MOD** PS-4	**HIGH** PS-4

PS-5 PERSONNEL TRANSFER

Control: The organization reviews information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and initiates appropriate actions.

Supplemental Guidance: Appropriate actions that may be required include: (i) returning old and issuing new keys, identification cards, building passes; (ii) closing old accounts and establishing new accounts; (iii) changing system access authorizations; and (iv) providing for access to official records created or controlled by the employee at the old work location and in the old accounts.

Control Enhancements: None.

LOW PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Control: The organization completes appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and reviews/updates the agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

Control Enhancements: None.

LOW PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization establishes personnel security requirements including security roles and responsibilities for third-party providers and monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents. NIST Special Publication 800-35 provides guidance on information technology security services.

Control Enhancements: None.

LOW PS-7	**MOD** PS-7	**HIGH** PS-7

PS-8 PERSONNEL SANCTIONS

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures for the organization.

Control Enhancements: None.

LOW PS-8	**MOD** PS-8	**HIGH** PS-8

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: The risk assessment policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publications 800-30 provides guidance on the assessment of risk. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.

Supplemental Guidance: The applicable federal standard for security categorization of nonnational security information and information systems is FIPS 199. The organization conducts FIPS 199 security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information security officer, information system owners, and information owners. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and restricting or prohibiting network access in accordance with an organizational assessment of risk. NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system. Related security controls: MP-4, SC-7.

Control Enhancements: None.

LOW RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT

Control: The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

Supplemental Guidance: Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system. The organization also considers potential impacts to other organizations and, in accordance with the USA PATRIOT Act and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems. NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.

Control Enhancements: None.

LOW RA-3	**MOD** RA-3	**HIGH** RA-3

RA-4 RISK ASSESSMENT UPDATE

Control: The organization updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

Supplemental Guidance: The organization develops and documents specific criteria for what is considered significant change to the information system. NIST Special Publication 800-30 provides guidance on conducting risk assessment updates.

Control Enhancements: None.

LOW RA-4	**MOD** RA-4	**HIGH** RA-4

RA-5 VULNERABILITY SCANNING

Control: The organization scans for vulnerabilities in the information system [*Assignment: organization-defined frequency*] or when significant new vulnerabilities potentially affecting the system are identified and reported.

Supplemental Guidance: Vulnerability scanning is conducted using appropriate scanning tools and techniques. The organization trains selected personnel in the use and maintenance of vulnerability scanning tools and techniques. Vulnerability scans are scheduled and/or random in accordance with organizational policy and assessment of risk. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems. Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools for applications, source code reviews, static analysis of source code). NIST Special Publication 800-42 provides guidance on network security testing. NIST Special Publication 800-40 (Version 2) provides guidance on patch and vulnerability management.

Control Enhancements:

(1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

(2) The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when significant new vulnerabilities are identified and reported.

(3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of scan coverage, including vulnerabilities checked and information system components scanned.

LOW Not Selected	**MOD** RA-5	**HIGH** RA-5 (1) (2)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: The system and services acquisition policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Control: The organization determines, documents, and allocates as part of its capital planning and investment control process, the resources required to adequately protect the information system.

Supplemental Guidance: The organization includes the determination of security requirements for the information system in mission/business case planning and establishes a discrete line item for information system security in the organization's programming and budgeting documentation. NIST Special Publication 800-65 provides guidance on integrating security into the capital planning and investment control process.

Control Enhancements: None.

LOW SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 LIFE CYCLE SUPPORT

Control: The organization manages the information system using a system development life cycle methodology that includes information security considerations.

Supplemental Guidance: NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

Control Enhancements: None.

LOW SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITIONS

Control: The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

Supplemental Guidance:

Solicitation Documents

The solicitation documents (e.g., Requests for Proposals) for information systems and services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. NIST Special Publication 800-36 provides guidance on the selection of information security products. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on security considerations in the system development life cycle.

Information System Documentation

The solicitation documents include requirements for appropriate information system documentation. The documentation addresses user and systems administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the FIPS 199 security category for the information system.

Use of Tested, Evaluated, and Validated Products

NIST Special Publication 800-23 provides guidance on the acquisition and use of tested/evaluated information technology products.

Configuration Settings and Implementation Guidance

The information system required documentation includes security configuration settings and security implementation guidance. OMB FISMA reporting instructions provide guidance on configuration requirements for federal information systems. NIST Special Publication 800-70 provides guidance on configuration settings for information technology products.

Control Enhancements:

(1) The organization requires in solicitation documents that appropriate documentation be provided describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

(2) The organization requires in solicitation documents that appropriate documentation be provided describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

LOW SA-4	**MOD** SA-4 (1)	**HIGH** SA-4 (1)

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization obtains, protects as required, and makes available to authorized personnel, adequate documentation for the information system.

Supplemental Guidance: Documentation includes administrator and user guides with information on: (i) configuring, installing, and operating the information system; and (ii) effectively using the system's security features. When adequate information system documentation is either unavailable or non existent (e.g., due to the age of the system or lack of support from the vendor/manufacturer), the organization documents attempts to obtain such documentation and provides compensating security controls, if needed.

Control Enhancements:

(1) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

(2) The organization includes, in addition to administrator and user guides, documentation, if available from the vendor/manufacturer, describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).

LOW SA-5	**MOD** SA-5 (1)	**HIGH** SA-5 (1) (2)

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: The organization complies with software usage restrictions.

Supplemental Guidance: Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licenses, the organization employs tracking systems to control copying and distribution. The organization controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Control Enhancements: None.

LOW SA-6	**MOD** SA-6	**HIGH** SA-6

SA-7 USER INSTALLED SOFTWARE

Control: The organization enforces explicit rules governing the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software that is free only for personal, not government use, and software whose pedigree with regard to being potentially malicious is unknown or suspect).

Control Enhancements: None.

LOW SA-7	**MOD** SA-7	**HIGH** SA-7

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization designs and implements the information system using security engineering principles.

Supplemental Guidance: NIST Special Publication 800-27 provides guidance on engineering principles for information system security. The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the system.

Control Enhancements: None.

LOW Not Selected	**MOD** SA-8	**HIGH** SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization: (i) requires that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitors security control compliance.

Supplemental Guidance: An external information system service is a service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. Ultimately, the responsibility for adequately mitigating risks to the organization's operations and assets, and to individuals, arising from the use of external information system services remains with the authorizing official. Authorizing officials must require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information system security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk to its operations and assets, or to individuals. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance. NIST Special Publication 800-35 provides guidance on information technology security services. NIST Special Publication 800-64 provides guidance on the security considerations in the system development life cycle.

Control Enhancements: None.

LOW SA-9	**MOD** SA-9	**HIGH** SA-9

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.

Supplemental Guidance: This control also applies to the development actions associated with information system changes.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** SA-10

SA-11 DEVELOPER SECURITY TESTING

Control: The organization requires that information system developers create a security test and evaluation plan, implement the plan, and document the results.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security certification and accreditation process for the delivered information system. Related security controls: CA-2, CA-4.

Control Enhancements: None.

LOW Not Selected	**MOD** SA-11	**HIGH** SA-11

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: The system and communications protection policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SC-1	**MOD** SC-1	**HIGH** SC-1

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process.

Control Enhancements:

(1) The information system employs underlying hardware separation mechanisms to facilitate security function isolation.

(2) The information system isolates critical security functions (i.e., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.

(3) The information system minimizes the number of nonsecurity functions included within the isolation boundary containing security functions.

(4) The information system security functions are implemented as largely independent modules that avoid unnecessary interactions between modules.

(5) The information system security functions are implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

LOW Not Selected	**MOD** Not Selected	**HIGH** SC-3

SC-4 INFORMATION REMNANCE

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: Control of information system remnance, sometimes referred to as object reuse, or data remnance, prevents information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Information systems that are publicly accessible can be protected by employing increased capacity and bandwidth combined with service redundancy.

Control Enhancements:

(1) The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.

(2) The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.

LOW SC-5	**MOD** SC-5	**HIGH** SC-5

SC-6 RESOURCE PRIORITY

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-7 BOUNDARY PROTECTION

Control: The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.

Supplemental Guidance: Any connections to the Internet, or other external networks or information systems, occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). Information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, the organization considers partitioning higher-impact information systems into separate physical domains (or environments) and applying the concepts of managed interfaces described above to restrict or prohibit network access in accordance with an organizational assessment of risk. FIPS 199 security categorization guides the selection of appropriate candidates for domain partitioning.

The organization carefully considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-77 provides guidance on virtual private networks. Related security controls: MP-4, RA-2.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate, physical network interfaces.

Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

(2) The organization prevents public access into the organization's internal networks except as appropriately mediated.

(3) The organization limits the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.

(4) The organization implements a managed interface (boundary protection devices in an effective security architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.

(5) The information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

(6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

LOW SC-7	**MOD** SC-7 (1) (2) (3) (4) (5)	**HIGH** SC-7 (1) (2) (3) (4) (5) (6)

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission integrity using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission integrity using IPsec. NIST Special Publication 800-81 provides guidance on Domain Name System (DNS) message authentication and integrity verification. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

LOW Not Selected	**MOD** SC-8	**HIGH** SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. NIST Special Publication 800-52 provides guidance on protecting transmission confidentiality using Transport Layer Security (TLS). NIST Special Publication 800-77 provides guidance on protecting transmission confidentiality using IPsec. NSTISSI No. 7003 contains guidance on the use of Protective Distribution Systems. Related security control: AC-17.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems.

LOW Not Selected	**MOD** SC-9	**HIGH** SC-9 (1)

SC-10 NETWORK DISCONNECT

Control: The information system terminates a network connection at the end of a session or after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: The organization applies this control within the context of risk management that considers specific mission or operational requirements.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*].

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: When cryptography is required and employed within the information system, the organization establishes and manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

Supplemental Guidance: NIST Special Publication 800-56 provides guidance on cryptographic key establishment. NIST Special Publication 800-57 provides guidance on cryptographic key management.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-12	**HIGH** SC-12

SC-13 USE OF CRYPTOGRAPHY

Control: For information requiring cryptographic protection, the information system implements cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Supplemental Guidance: The applicable federal standard for employing cryptography in nonnational security information systems is FIPS 140-2 (as amended). Validation certificates issued by the NIST Cryptographic Module Validation Program (including FIPS 140-1, FIPS 140-2, and future amendments) remain in effect and the modules remain available for continued use and purchase until a validation certificate is specifically revoked. NIST Special Publications 800-56 and 800-57 provide guidance on cryptographic key establishment and cryptographic key management. Additional information on the use of validated cryptography is available at http://csrc.nist.gov/cryptval.

Control Enhancements: None.

LOW SC-13	**MOD** SC-13	**HIGH** SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

Control: The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: None.

Control Enhancements: None.

LOW SC-14	**MOD** SC-14	**HIGH** SC-14

SC-15 COLLABORATIVE COMPUTING

Control: The information system prohibits remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users.

Supplemental Guidance: Collaborative computing mechanisms include, for example, video and audio conferencing capabilities. Explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

Control Enhancements:

(1) The information system provides physical disconnect of camera and microphone in a manner that supports ease of use.

LOW Not Selected	**MOD** SC-15	**HIGH** SC-15

SC-16 TRANSMISSION OF SECURITY PARAMETERS

Control: The information system reliably associates security parameters with information exchanged between information systems.

Supplemental Guidance: Security parameters include, for example, security labels and markings. Security parameters may be explicitly or implicitly associated with the information contained within the information system.

Control Enhancements: None.

LOW Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each agency either establishes an agency certification authority cross-certified with the Federal Bridge Certification Authority at medium assurance or higher or uses certificates from an approved, shared service provider, as required by OMB Memorandum 05-24. NIST Special Publication 800-32 provides guidance on public key technology. NIST Special Publication 800-63 provides guidance on remote electronic authentication.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-17	**HIGH** SC-17

SC-18 MOBILE CODE

Control: The organization: (i) establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Control procedures prevent the development, acquisition, or introduction of unacceptable mobile code within the information system. NIST Special Publication 800-28 provides guidance on active content and mobile code.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-18	**HIGH** SC-18

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization: (i) establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: NIST Special Publication 800-58 provides guidance on security considerations for VoIP technologies employed in information systems.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-19	**HIGH** SC-19

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system that provides name/address resolution service provides additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer resource records.

LOW Not Selected	**MOD** SC-20	**HIGH** SC-20

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: The information system that provides name/address resolution service for local clients performs data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

Supplemental Guidance: A resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients and authoritative DNS servers are examples of authoritative sources. NIST Special Publication 800-81 provides guidance on secure domain name system deployment.

Control Enhancements:

(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.

Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.

LOW Not Selected	**MOD** Not Selected	**HIGH** SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault tolerant and implement role separation.

Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). If organizational information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, authoritative DNS servers with two roles (internal and external) are established. The DNS server with the internal role provides name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources. The list of clients who can access the authoritative DNS server of a particular role is also specified. NIST Special Publication 800-81 provides guidance on secure DNS deployment.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services). NIST Special Publication 800-52 provides guidance on the use of transport layer security (TLS) mechanisms. NIST Special Publication 800-77 provides guidance on the deployment of IPsec virtual private networks (VPNs) and other methods of protecting communications sessions. NIST Special Publication 800-95 provides guidance on secure web services.

Control Enhancements: None.

LOW Not Selected	**MOD** SC-23	**HIGH** SC-23

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Supplemental Guidance: The system and information integrity policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.

Control Enhancements: None.

LOW SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION

Control: The organization identifies, reports, and corrects information system flaws.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws). The organization (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) promptly installs newly released security relevant patches, service packs, and hot fixes, and tests patches, service packs, and hot fixes for effectiveness and potential side effects on the organization's information systems before installation. Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling are also addressed expeditiously. Flaw remediation is incorporated into configuration management as an emergency change. NIST Special Publication 800-40, provides guidance on security patch installation and patch management. Related security controls: CA-2, CA-4, CA-7, CM-3, IR-4, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs updates automatically.

(2) The organization employs automated mechanisms to periodically and upon demand determine the state of information system components with regard to flaw remediation.

LOW SI-2	**MOD** SI-2 (2)	**HIGH** SI-2 (1) (2)

SI-3 MALICIOUS CODE PROTECTION

Control: The information system implements malicious code protection.

Supplemental Guidance: The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities. The organization updates malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. The organization considers using malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). The organization also considers the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. NIST Special Publication 800-83 provides guidance on implementing malicious code protection.

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates malicious code protection mechanisms.

LOW SI-3	**MOD** SI-3 (1) (2)	**HIGH** SI-3 (1) (2)

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

Control: The organization employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

Supplemental Guidance: Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Monitoring devices are strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices are also deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices are used to track the impact of security changes to the information system. The granularity of the information collected is determined by the organization based upon its monitoring objectives and the capability of the information system to support such activities. Organizations consult appropriate legal counsel with regard to all information system monitoring activities. Organizations heighten the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information. NIST Special Publication 800-61 provides guidance on detecting attacks through various types of security technologies. NIST Special Publication 800-83 provides guidance on detecting malware-based attacks through malicious code protection software. NIST Special Publication 800-92 provides guidance on monitoring and analyzing computer security event logs. NIST Special Publication 800-94 provides guidance on intrusion detection and prevention. Related security control: AC-8.

Control Enhancements:

(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

(2) The organization employs automated tools to support near-real-time analysis of events.

(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.

(5) The information system provides a real-time alert when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].

LOW Not Selected	**MOD** SI-4 (4)	**HIGH** SI-4 (2) (4) (5)

SI-5 SECURITY ALERTS AND ADVISORIES

Control: The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

Supplemental Guidance: The organization documents the types of actions to be taken in response to security alerts/advisories. The organization also maintains contact with special interest groups (e.g., information security forums) that: (i) facilitate sharing of security-related information (e.g., threats, vulnerabilities, and latest security technologies); (ii) provide access to advice from security professionals; and (iii) improve knowledge of security best practices. NIST Special Publication 800-40 provides guidance on monitoring and distributing security alerts and advisories.

Control Enhancements:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

LOW SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system verifies the correct operation of security functions [*Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator, shuts the system down, restarts the system*] when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required.

Control Enhancements:

(1) The organization employs automated mechanisms to provide notification of failed automated security tests.

(2) The organization employs automated mechanisms to support management of distributed security testing.

LOW Not Selected	**MOD** Not Selected	**HIGH** SI-6

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The information system detects and protects against unauthorized changes to software and information.

Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Control Enhancements:

(1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the system.

(2) The organization employs automated tools that provide notification to appropriate individuals upon discovering discrepancies during integrity verification.

(3) The organization employs centrally managed integrity verification tools.

LOW Not Selected	**MOD** Not Selected	**HIGH** SI-7 (1) (2)

SI-8 SPAM PROTECTION

Control: The information system implements spam protection.

Supplemental Guidance: The organization employs spam protection mechanisms at critical information system entry points (e.g., firewalls, electronic mail servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the spam protection mechanisms to detect and take appropriate action on unsolicited messages transported by electronic mail, electronic mail attachments, Internet accesses, or other common means. Consideration is given to using spam protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations). NIST Special Publication 800-45 provides guidance on electronic mail security.

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The information system automatically updates spam protection mechanisms.

LOW Not Selected	**MOD** SI-8	**HIGH** SI-8 (1)

SI-9 INFORMATION INPUT RESTRICTIONS

Control: The organization restricts the capability to input information to the information system to authorized personnel.

Supplemental Guidance: Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-9	**HIGH** SI-9

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY

Control: The information system checks information for accuracy, completeness, validity, and authenticity.

Supplemental Guidance: Checks for accuracy, completeness, validity, and authenticity of information are accomplished as close to the point of origin as possible. Rules for checking the valid syntax of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands. The extent to which the information system is able to check the accuracy, completeness, validity, and authenticity of information is guided by organizational policy and operational requirements.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-10	**HIGH** SI-10

SI-11 ERROR HANDLING

Control: The information system identifies and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.

Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. Error messages are revealed only to authorized personnel. Error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries. Sensitive information (e.g., account numbers, social security numbers, and credit card numbers) are not listed in error logs or associated administrative messages. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-11	**HIGH** SI-11

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: None.

Control Enhancements: None.

LOW Not Selected	**MOD** SI-12	**HIGH** SI-12

APPENDIX G

SECURITY CONTROL MAPPINGS

RELATIONSHIP OF SECURITY CONTROLS TO OTHER STANDARDS AND CONTROL SETS

The mapping table in this appendix provides organizations with a *general* indication of Special Publication 800-53 security control coverage with respect to other frequently referenced security control standards and control sets.[51] The security control mappings are not exhaustive and are based on a broad interpretation and general understanding of the control sets being compared. The mappings are created by using the primary security topic identified in each of the Special Publication 800-53 security controls and associated control enhancements (if any) and searching for a similar security topic in the other referenced security control standards and control sets. Security controls with similar functional meaning are included in the mapping table. For example, Special Publication 800-53 contingency planning and ISO/IEC 17799[52] business continuity were deemed to have similar, but not exactly the same, functionality. In some instances, similar topics are addressed in the security control sets but provide a different context, perspective, or scope. For example, Special Publication 800-53 addresses information flow broadly in terms of assigned authorizations for controlling access between source and destination objects, whereas ISO/IEC 17799 addresses the information flow more narrowly as it applies to interconnected network domains. And finally, the following cautionary notes are in order:

- The granularity of the security control sets being compared is not always the same. This difference in granularity makes the security control mappings less precise in some instances. Therefore, the mappings should not be used as a "checklist" for the express purpose of comparing security capabilities or security implementations across information systems assessed against different control sets.
- Some of the control sets referenced in this appendix (e.g., Department of Defense Instruction 8500.2) are organized into groups of security controls with each group reflecting different levels of protection. When the security control groups reflect a hierarchical enhancement of another group, only the paragraph reference from the lowest hierarchical group where the security topic first occurred is listed in the mapping column.

Organizations are encouraged to use the mapping table only as a starting point for conducting further analyses and interpretation of control similarity and associated coverage when comparing disparate control sets.

[51] The security control mapping table includes references to: (i) ISO/IEC 17799: 2005, *Code of Practice for Information Security Management*; (ii) NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*; (iii) GAO, *Federal Information System Controls Audit Manual*; (iv) Director of Central Intelligence Directive 6/3 Policy and Manual, *Protecting Sensitive Compartmented Information within Information Systems*; and (v) Department of Defense Instruction 8500.2, *Information Assurance Implementation.* The designations in the respective columns indicate the paragraph identifier(s) or number(s) in the above documents where the security controls, control objectives, or associated implementation guidance may be found.

[52] ISO/IEC 17799, *Code of Practice for Information Security Management,* is expected to be renamed to ISO 27002 consistent with the new designations for the ISO series of information security publications. ISO/IEC 17799 security controls are also referenced in ISO/IEC 27001:2005 *Specification for an Information Security Management System.*

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
Access Control						
AC-1	Access Control Policy and Procedures	11.1.1 11.4.1 15.1.1	15. 16.	---	ECAN-1 ECPA-1 PRAS-1 DCAR-1	2.B.4.e(5) 4.B.1.a(1)(b)
AC-2	Account Management	6.2.2 6.2.3 8.3.3 11.2.1 11.2.2 11.2.4 11.7.2	6.1.8 15.1.1 15.1.4 15.1.5 15.1.8 15.2.2 16.1.3 16.1.5 16.2.12	AC-2.1 AC-2.2 AC-3.2 SP-4.1	IAAC-1	4.B.2.a(3)
AC-3	Access Enforcement	11.2.4 11.4.5	10.1.2 15.1.1 16.1.1 16.1.2 16.1.3 16.1.7 16.1.9 16.2.1 16.2.7 16.2.10 16.2.11 16.2.15	AC-2 AC-3.2	DCFA-1 ECAN-1 EBRU-1 PRNK-1 ECCD-1 ECSD-2	Discretionary Access Control (DAC): 4.B.2.a(2) Mandatory Access Control (MAC): 4.B.4.a(3)
AC-4	Information Flow Enforcement	10.6.2 11.4.5 11.4.6 11.4.7	---	---	EBBD-1 EBBD-2	4.B.3.a(3) 7.B.3.g
AC-5	Separation of Duties	10.1.3 10.6.1 10.10.1	6.1.1 6.1.2 6.1.3 15.2.1 16.1.2 17.1.5	AC-3.2 SD-1.2	ECLP-1	2.A.1 4.B.3.a(18)
AC-6	Least Privilege	11.2.2	16.1.2 16.1.3 17.1.5	AC-3.2	ECLP-1	4.B.2.a(10)
AC-7	Unsuccessful Login Attempts	11.5.1	15.1.14	AC-3.2	ECLO-1	4.B.2.a(17)(c)-(d)
AC-8	System Use Notification	11.5.1 15.1.5	16.2.13 16.3.1 17.1.9	AC-3.2	ECWM-1	4.B.1.a(6)
AC-9	Previous Logon Notification	11.5.1	---	AC-3.2	ECLO-2	---

[53] References in this column are to both DCI Directive 6/3 and to its Manual (Administrative update, December 2003). Paragraphs cited from the Directive are preceded by "DCID" and where there are also references for the same control from the Manual, these are preceded by "Manual." Where only paragraph numbers appear, they are references to the Manual. References to paragraphs in the Manual should be construed to encompass all subparagraphs related to those paragraphs. It should also be noted that Special Publication 800-53 contains a set of security controls that cover personnel, physical, and technical security measures, and therefore, the scope of the publication is broader than DCID 6/3. Some of the controls in Special Publication 800-53 are explicitly not included in DCID 6/3 because they are addressed in other DCID and Intelligence Community (IC) policy documents. The difference in scope/breadth between Special Publication 800-53 and DCID 6/3 impacts the degree of correlation between the two documents. Thus, the lack of a "mapping" for a particular Special Publication 800-53 control to a DCID 6/3 requirement does not mean that there is no similar IC requirement. The IC Translation Review Board provided information for the DCID 6/3 mapping.

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
AC-10	Concurrent Session Control	---	---	---	ECLO-1	4.B.2.a(17)(a)
AC-11	Session Lock	11.3.2	16.1.4	AC-3.2	PESL-1	4.B.1.a(5)
AC-12	Session Termination	11.3.2 11.5.5	16.1.4 16.2.6	AC-3.2	---	4.B.2.a(17)(b)
AC-13	Supervision and Review—Access Control	10.10.2 11.2.4	7.1.10 11.2.2 16.1.10 16.2.5 17.1.6 17.1.7	AC-4 AC-4.3 SS-2.2	ECAT-1 ECAT-2 E3.3.9	2.B.7.c 4.B.3.a(8)(b)
AC-14	Permitted Actions without Identification or Authentication	---	16.2.12	---	---	7.D.3.a
AC-15	Automated Marking	7.2.2	8.2.4 16.1.6	AC-3.2	ECML-1	4.B.2.a(11)
AC-16	Automated Labeling	7.2.2	16.1.6	AC-3.2	ECML-1	4.B.1.a(3) 4.B.4.a(15) 4.B.4.a(16)
AC-17	Remote Access	11.4.2 11.4.3 11.4.4	16.2.4 16.2.8	AC-3.2	EBRP-1 EBRU-1	4.B.1.a(1)(b) 4.B.3.a(11) 7.D.2.e
AC-18	Wireless Access Restrictions	11.4.2 11.7.1 11.7.2	---	---	ECCT-1 ECWN-1	4.B.1.a(8) 5.B.3.a(11)
AC-19	Access Control for Portable and Mobile Devices	11.7.1	7.3.1 7.3.2	---	ECWN-1	8.B.6.c 9.G.4
AC-20	Use of External Information Systems	6.1.4 9.2.5 11.7.1	10.2.13	---	---	8.B.6.c
Awareness and Training						
AT-1	Security Awareness and Training Policy and Procedures	5.1.1 8.2.2 15.1.1	13.	---	PRTN-1 DCAR-1	DCID: B.3.c Manual: 2.B.2.b(8); 2.B.4.e(6)
AT-2	Security Awareness	6.2.3 8.2.2 10.4.1 11.7.1 13.1.1 14.1.4 15.1.4	13.1.4 13.1.5	---	PRTN-1	8.B.1
AT-3	Security Training	8.2.2 10.3.2 11.7.1 13.1.1 14.1.4	13.1 13.1.3 13.1.5	---	PRTN-1	8.B.1
AT-4	Security Training Records	---	13.1.2	---	---	8.B.1
AT-5	Contacts with Security Groups and Associations	6.1.7	---	---	---	---
Audit and Accountability						
AU-1	Audit and Accountability Policy and Procedures	10.10 15.1.1	17.	---	ECAT-1 ECTB-1 DCAR-1	DCID: B.2.d Manual: 2.B.4.e(5); 4.B.2.a(4)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
AU-2	Auditable Events	10.10.1	17.1.1 17.1.2 17.1.4	---	ECAR-3	4.B.2.a(4)(d)
AU-3	Content of Audit Records	10.10.1 10.10.4	17.1.1	---	ECAR-1 ECAR-2 ECAR-3 ECLC-1	4.B.2.a(4)(a) 4.B.2.a(5)(a)
AU-4	Audit Storage Capacity	10.10.3	---	---	---	5.B.2.a(5)(a)(1)
AU-5	Response to Audit Processing Failures	10.10.3	---	---	---	4.B.4.a(9)(d)
AU-6	Audit Monitoring, Analysis, and Reporting	10.10.2 10.10.4 13.2.1	16.2.5 17.1.7 17.1.8	AC-4.3	ECAT-1 E3.3.9	4.B.4.a(10)
AU-7	Audit Reduction and Report Generation	10.10.3	17.1.2 17.1.7	---	ECRG-1	4.B.3.a(6)
AU-8	Time Stamps	10.10.6	---	---	ECAR-1	4.B.2.a(4)(a)
AU-9	Protection of Audit Information	10.10.3 15.1.3 15.3.2	17.1.3 17.1.4	---	ECTP-1	4.B.2.a(4)(b)
AU-10	Non-repudiation	10.8.2 10.9.1 12.3.1	15.1.2 17.1.1	---	DCNR-1	5.B.3.a(8)
AU-11	Audit Record Retention	10.10.1 15.1.3	17.1.4	---	ECRR-1	4.B.2.a(4)(c)
Certification, Accreditation, and Security Assessments						
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	6.1.4 10.3.2 15.1.1	2. 4.	---	DCAR-1 DCII-1	DCID: B.3 Manual: 2.B.2.b(1)
CA-2	Security Assessments	6.1.8 15.2.1 15.2.2	2.1.1 2.1.3 2.1.4	SP-5.1	DCII-1 ECMT-1 PEPS-1 E3.3.10	DCID: B.2.b; B.3.a Manual: 4.B.2.b(6); 5.B.1.b(1); 9.B.1; 9.B.4
CA-3	Information System Connections	10.6.2 10.9.1 11.4.5 11.4.6 11.4.7	1.1.1 3.2.9 4.1.8 12.2.3	CC-2.1	DCID-1 EBCR-1 EBRU-1 EBPW-1 ECIC-1	9.B.3 9.D.3.c
CA-4	Security Certification	10.3.2	2.1.2 3.2.3 3.2.5 3.2.6 4.1.1 4.1.6 11.2.8 12.2.5	CC-2.1	DCAR-1 5.7.5	DCID: B.3 Manual: 4.B.3.b(8); 9.E.2.a(2); 9.E.2.a(3)
CA-5	Plan of Action and Milestones	15.2.1	1.1.5 1.2.3 2.2.1 4.2.1	SP-5.1 SP-5.2	5.7.5	9.E.2.a(3)(a)
CA-6	Security Accreditation	10.3.2	3.2.7 12.2.5	---	5.7.5	DCID: B.3 Manual: 9.D.3; 9.D.4

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
CA-7	Continuous Monitoring	15.2.1 15.2.2	10.2.1	---	DCCB-1 DCPR-1 E3.3.9	DCID: B.2.d; Manual: 2.B.4.e(7); 2.B.5.c(10); 5.B.2.b(2); 9.B.1; 9.D.7
Configuration Management						
CM-1	Configuration Management Policy and Procedures	12.4.1 12.5.1 15.1.1	---	---	DCCB-1 DCPR-1 DCAR-1 E3.3.8	DCID: B.2.a Manual: 2.B.4.e(5); 5.B.2.a(5)
CM-2	Baseline Configuration	7.1.1 15.1.2	1.1.1 3.1.9 10.2.7 10.2.9 12.1.4	CC-2.3 CC-3.1 SS-1.2	DCHW-1 DCSW-1	2.B.7.c(7) 4.B.1.c(3) 4.B.2.b(6)
CM-3	Configuration Change Control	10.1.2 10.2.3 12.4.1 12.5.1 12.5.2 12.5.3	3.1.4 10.2.2 10.2.3 10.2.8 10.2.10 10.2.11	SS-3.2 CC-2.2	DCPR-1	2.B.7.c(7) 4.B.1.c(3) 4.B.2.b(6) 5.B.2.a(5)
CM-4	Monitoring Configuration Changes	10.1.2	10.2.1 10.2.4	SS-3.1 SS-3.2 CC-2.1	DCPR-1 E3.3.8	2.B.7.c(7) 4.B.1.c(3) 5.B.2.b(2) 8.B.8.c(7)
CM-5	Access Restrictions for Change	11.6.1	6.1.3 6.1.4 10.1.1 10.1.4 10.1.5	SD-1.1 SS-1.2 SS-2.1	DCPR-1 ECSD-2	5.B.3.a(2)(b)
CM-6	Configuration Settings	---	10.2.6 10.3.1 16.2.2 16.2.3 16.2.11	---	DCSS-1 ECSC-1 E3.3.8	4.B.2.a(10)
CM-7	Least Functionality	---	10.3.1	---	DCPP-1 ECIM-1 ECVI-1 E3.3.8	4.B.2.a(10) 7.D.2.b
CM-8	Information System Component Inventory	7.1.1 15.1.2	1.1.1 3.1.9 10.2.7 10.2.9 12.1.4	CC-2.3 CC-3.1 SS-1.2	DCHW-1 DCSW-1	2.B.7.c(7) 4.B.1.c(3) 4.B.2.b(6)
Contingency Planning						
CP-1	Contingency Planning Policy and Procedures	5.1.1 10.4.1 14.1.1 14.1.3 15.1.1	9.	---	COBR-1 DCAR-1	2.B.4.e(5) 6.B.1.a(1)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
CP-2	Contingency Plan	10.3.2 10.4.1 10.8.5 14.1.3 14.1.4	4.1.4 9.1.1 9.2 9.2.1 9.2.2 9.2.3 9.2.10 12.1.8 12.2.2	SC-3.1 SC-1.1	CODP-1 COEF-1	6.B.2.b(1)
CP-3	Contingency Training	14.1.3 14.1.4	9.3.2	SC-2.3	PRTN-1	8.B.1
CP-4	Contingency Plan Testing and Exercises	10.5.1 14.1.5	4.1.4 9.3.3	SC-3.1	COED-1	6.B.3.b(2)(b)
CP-5	Contingency Plan Update	14.1.3 14.1.5	9.3.1 9.3.3 10.2.12	SC-2.1 SC-3.1	DCAR-1	6.B.3.b(2)
CP-6	Alternate Storage Site	10.5.1	9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1	CODB-2	6.B.2.a(2) 6.B.3.a(2)(d)
CP-7	Alternate Processing Site	14.1.4	9.1.3 9.2.4 9.2.5 9.2.7 9.2.9	SC-2.1 SC-3.1	COAS-1 COEB-1 COSP-1 COSP-2	6.B.3.a(2)(d)
CP-8	Telecommunications Services	14.1.4	---	---	---	6.B.2.a(4)
CP-9	Information System Backup	10.5.1 11.7.1	9.1.1 9.2.6 9.2.9 9.3.1 12.1.9	SC-2.1	CODB-1 CODB-2 COSW-1	6.B.1.a(2)
CP-10	Information System Recovery and Reconstitution	14.1.4	9.2.8	SC-2.1	COTR-1 ECND-1	4.B.1.a(4) 6.B.1.a(1) 6.B.2.a(3)(d)
Identification and Authentication						
IA-1	Identification and Authentication Policy and Procedures	15.1.1	11.2.3	---	IAIA-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)
IA-2	User Identification and Authentication	11.2.3 11.4.2 11.5.2	15.1	---	IAIA-1	4.B.2.a(7)
IA-3	Device Identification and Authentication	11.4.2 11.4.3 11.7.1	16.2.7	---	---	4.B.5.a(14)
IA-4	Identifier Management	11.2.3 11.5.2	15.1.1 15.2.2 15.1.8	AC-2.1 AC-3.2 SP-4.1	IAGA-1 IAIA-1	4.B.1.a(2)
IA-5	Authenticator Management	11.5.2 11.5.3	15.1.6 15.1.7 15.1.9 15.1.10 15.1.11 15.1.12 15.1.13 16.1.3 16.2.3	AC-3.2	IAKM-1 IATS-1	4.B.2.a(7) 4.B.3.a(11)
IA-6	Authenticator Feedback	11.5.1	---	---	---	4.B.2.a(7)(g)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
IA-7	Cryptographic Module Authentication	---	16.1.7	---	---	1.G
Incident Response						
IR-1	Incident Response Policy and Procedures	10.4.1 13.1 13.2.1 15.1.1	14.	---	VIIR-1 DCAR-1	DCID: B.2.c; C.4 Manual: 2.B.4.e(5); 2.B.2.b(6); 2.B.6.c(10); 8.B.7
IR-2	Incident Response Training	13.1.1	14.1.4	SP-3.4	VIIR-1	8.B.1.b(1)(f) 8.B.1.c(1)(e) 8.B.1.c(2)(c)
IR-3	Incident Response Testing and Exercises	14.1.5	---	---	VIIR-1	8.B.7
IR-4	Incident Handling	6.1.6 13.2.1 13.2.2	2.1.5 14.1.1 14.1.2 14.1.6	SP-3.4	VIIR-1 E3.3.9	8.B.7 9.B.2.e
IR-5	Incident Monitoring	---	14.1.3	---	VIIR-1	8.B.7.a
IR-6	Incident Reporting	6.1.6 6.2.2 6.2.3 13.1.1 13.1.2	14.1.2 14.1.3 14.2.1 14.2.2 14.2.3	---	VIIR-1 E3.3.9	8.B.7
IR-7	Incident Response Assistance	14.1.3	8.1.1 14.1.1	SP-3.4	---	8.B.7.c
Maintenance						
MA-1	System Maintenance Policy and Procedures	10.1.1 15.1.1	10.	---	PRMP-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 6.B.2.a(5)
MA-2	Controlled Maintenance	9.2.4	10.1.1 10.1.3 10.2.1	SS-3.1	---	6.B.2.a(5) 8.B.8.c
MA-3	Maintenance Tools	---	10.1.3 11.2.4	---	---	6.B.3.a(5) 8.B.8.c(4) 8.B.8.c(5)
MA-4	Remote Maintenance	11.4.4	10.1.1 17.1.1	SS-3.1	EBRP-1	8.B.8.d
MA-5	Maintenance Personnel	6.2.3 9.2.4	10.1.1 10.1.3	SS-3.1	PRMP-1	8.B.8.a
MA-6	Timely Maintenance	---	9.1.2	SC-1.2	COMS-1 COSP-1	6.B.2.a(5)
Media Protection						
MP-1	Media Protection Policy and Procedures	10.1.1 10.7 15.1.1 15.1.3	8.2	---	PESP-1 DCAR-1	DCID: B.2.a Manual: 2.B.6.c(7); 8.B.2
MP-2	Media Access	10.7.3	8.2.1 8.2.2 8.2.3 8.2.6 8.2.7	---	PEDI-1 PEPF-1	2.B.9.b(4) 4.B.1.a(1) 4.B.1.a(7)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
MP-3	Media Labeling	7.2.2 10.7.3 10.8.2 15.1.3	8.2.5 8.2.6 10.2.9	---	ECML-1	2.B.9.b(4) 8.B.2.a 8.B.2.c
MP-4	Media Storage	10.7.1 10.7.2 10.7.3 10.7.4 15.1.3	7.1.4 8.2.1 8.2.2 8.2.9 10.1.2	AC-3.1	PESS-1	2.B.9.b(4) 4.B.1.a(7)
MP-5	Media Transport	10.8.3	8.2.2 8.2.4	---	---	2.B.9.b(4)
MP-6	Media Sanitization and Disposal	9.2.6 10.7.1 10.7.2	3.2.11 3.2.12 3.2.13 8.2.8 8.2.9 8.2.10	AC-3.4	PECS-1 PEDD-1	8.B.5 2.B.9.b(4) 8.B.5.a(4) 8.B.5.d 8.B.5.e
Physical and Environmental Protection						
PE-1	Physical and Environmental Protection Policy and Procedures	15.1.1	7.		PETN-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 8.D
PE-2	Physical Access Authorizations	9.1.2 9.1.6	7.1.1 7.1.2	AC-3.1	PECF-1	4.B.1.a(1) 8.E
PE-3	Physical Access Control	9.1.1 9.1.2 9.1.5 9.1.6 10.5.1	7.1.1 7.1.2 7.1.5 7.1.6 7.1.8	AC-3.1	PEPF-1	4.B.1.a(1) 8.D.2 8.E
PE-4	Access Control for Transmission Medium	9.2.3	7.2.2 16.2.9	---	---	8.D.2 4.B.1.a(8)
PE-5	Access Control for Display Medium	9.1.2 11.3.3	7.2.1	---	PEDI-1 PEPF-1	8.C.2.a 8.D.2
PE-6	Monitoring Physical Access	9.1.2	7.1.9	AC-4	PEPF-2	4.B.1.a(1) 8.C.2.a 8.D.2
PE-7	Visitor Control	9.1.2	7.1.7 7.1.11	AC-3.1	PEVC-1	8.C.2.a 8.D.2 8.E
PE-8	Access Records	9.1.2	7.1.9	AC-4	PEPF-2 PEVC-1	8.C.2.a 8.D.2 8.E
PE-9	Power Equipment and Power Cabling	9.2.2 9.2.3	7.1.16	SC-2.2	---	8.D.2
PE-10	Emergency Shutoff	9.2.2	---	---	PEMS-1	8.D.2
PE-11	Emergency Power	9.2.2	7.1.18	SC-2.2	COPS-1 COPS-2 COPS-3	6.B.2.a(6) 6.B.2.a(7)
PE-12	Emergency Lighting	9.2.2	---	---	PEEL-1	8.D.2
PE-13	Fire Protection	9.1.4 9.2.1	7.1.12	SC-2.2	PEFD-1 PEFS-1	8.C.2.a 8.D.2
PE-14	Temperature and Humidity Controls	9.2.1 10.5.1 10.7.1	7.1.14 7.1.15	SC-2.2	PEHC-1 PETC-1	8.D.2

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
PE-15	Water Damage Protection	9.1.4 9.2.1	7.1.17	SC-2.2	---	8.C.2.a 8.D.2
PE-16	Delivery and Removal	9.1.6 9.2.7 10.7.1	7.1.3	AC-3.1	---	8.B.5.e
PE-17	Alternate Work Site	11.7.2	---	---	EBRU-1	---
PE-18	Location of Information System Components	9.2.1	---	---	---	---
PE-19	Information Leakage	---	---	---	---	---
Planning						
PL-1	Security Planning Policy and Procedures	6.1 15.1.1	5.	---	DCAR-1 E3.4.6	DCID: B.2.a Manual: 2.B.4.e(5)
PL-2	System Security Plan	6.1	4.1.5 5.1.1 5.1.2 12.2.1	SP-2.1	DCSD-1	1.F.6 2.B.6.c(3) 2.B.7.c(5) 9.E.2.a(1)(d) 9.F.2.a Appendix C
PL-3	System Security Plan Update	6.1	3.2.10 5.2.1	SP-2.1	5.7.5	2.B.7.c(5)
PL-4	Rules of Behavior	7.1.3 8.1.3 15.1.5	4.1.3 13.1.1	---	PRRB-1	2.B.9.b
PL-5	Privacy Impact Assessment	15.1.4	---	---	---	DCID: B.3.a Manual: 8.B.9
PL-6	Security-Related Activity Planning	15.3.1	---	---	---	---
Personnel Security						
PS-1	Personnel Security Policy and Procedures	8.1.1 15.1.1	6.	---	PRRB-1 DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5); 8.E
PS-2	Position Categorization	8.1.2	6.1.1 6.1.2	SD-1.2	---	8.E
PS-3	Personnel Screening	8.1.2	6.2.1 6.2.3	SP-4.1	PRAS-1	2.B.7.c(2) 2.B.8.b(5) 8.E
PS-4	Personnel Termination	8.1.3 8.3 11.2.1	6.1.7	SP-4.1	5.12.7	2.B.9.b(6) 4.B.2.a(3)(e) 8.E
PS-5	Personnel Transfer	8.3.1 8.3.3 11.2.1	6.1.7	SP-4.1	5.12.7	2.B.9.b(6)
PS-6	Access Agreements	6.1.5 8.1.3	6.1.5 6.2.2	SP-4.1	PRRB-1	1.E.2 8.E

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
PS-7	Third-Party Personnel Security	6.2.1 6.2.3 8.1.1 8.1.2 8.1.3 8.2.1 8.2.2 11.2.1	---	SP-4.1	5.7.10	1.A.1 8.D 8.E
PS-8	Personnel Sanctions	8.2.3 11.2.1	6.1.5	---	PRRB-1	4.B.2.a(3)(e) 8.E
Risk Assessment						
RA-1	Risk Assessment Policy and Procedures	4.1 15.1.1	1.	---	DCAR-1	DCID: B.3.a Manual: 2.B.4.e(5)
RA-2	Security Categorization	7.2.1	1.1.3 3.1.1	SP-1 AC-1.1 AC-1.2	E3.4.2	3.C 3.D 9.E.2.a(1)(a) 9.E.2.a(1)(d)
RA-3	Risk Assessment	4.0 4.1 4.2 6.2.1 10.10.2 10.10.5 12.5.1 12.6.1 14.1.1 14.1.2	1.1.2 1.1.4 1.1.5 1.1.6 1.2.1 1.2.2 1.2.3 3.1.7 3.1.8 4.1.7 7.1.13 7.1.19 12.2.4	SP-1	DCDS-1 DCII-1 E3.3.10	9.B
RA-4	Risk Assessment Update	4.1	1.1.2 4.1.2	SP-1	DCAR-1 DCII-1	9.B.4.f 9.D.1.d
RA-5	Vulnerability Scanning	12.6.1	10.3.2 14.2.1	---	ECMT-1 VIVM-1	4.B.3.a(8)(b) 4.B.3.b(6)(b) 9.B.4.e
System and Services Acquisition						
SA-1	System and Services Acquisition Policy and Procedures	12.1 15.1.1	3.	---	DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)
SA-2	Allocation of Resources	10.3.1	3.1.2 3.1.3 3.1.5 5.1.3	---	DCPB-1 E3.3.4	DCID: C.2.a Manual: 2.B.4.e(8)
SA-3	Life Cycle Support	---	3.1	---	5.8.1	DCID: B.2.a Manual: 9.E.2
SA-4	Acquisitions	12.1.1	3.1.6 3.1.7 3.1.10 3.1.11 3.1.12	---	DCAS-1 DCDS-1 DCIT-1 DCMC-1	DCID: B.2.a; C.2.a Manual: 9.B.4

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
SA-5	Information System Documentation	10.7.4	3.2.3 3.2.4 3.2.8 12.1.1 12.1.2 12.1.3 12.1.6 12.1.7	CC-2.1	DCCS-1 DCHW-1 DCID-1 DCSD-1 DCSW-1 ECND-1 DCFA-1	4.B.2.b(2) 4.B.2.b(3) 4.B.4.b(4) 9.C.3
SA-6	Software Usage Restrictions	15.1.2	10.2.10 10.2.13	SS-3.2 SP-2.1	DCPD-1	2.B.9.b(11)
SA-7	User Installed Software	15.1.2	10.2.10	SS-3.2	---	2.B.9.b(11)
SA-8	Security Engineering Principles	12.1	3.2.1	---	DCBP-1 DCCS-1 E3.4.4	1.H.1
SA-9	External Information System Services	6.2.1 6.2.3 10.2.1 10.2.2 10.6.2	12.2.3	---	DCDS-1 DCID-1 DCIT-1 DCPP-1	1.B.1 8.C.2 8.E
SA-10	Developer Configuration Management	12.5.1 12.5.2	---	SS-3.1 CC-3	---	4.B.4.b(4) 8.C.2.a
SA-11	Developer Security Testing	12.5.1 12.5.2	3.2.1 3.2.2 10.2.5 12.1.5	SS-3.1 CC-2.1	E3.4.4	4.B.4.b(4)
System and Communications Protection						
SC-1	System and Communications Protection Policy and Procedures	10.8.1 15.1.1	---	---	DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5)
SC-2	Application Partitioning	11.4.5	---	---	DCPA-1	4.B.3.b(6)(a) 4.B.4.b(8) 5.B.3.b(2)
SC-3	Security Function Isolation	11.4.5	---	---	DCSP-1	4.B.3.b(6)(a) 4.B.4.b(8) 5.B.3.b(1) 5.B.3.b(2)
SC-4	Information Remnance	10.8.1	---	AC-3.4	ECRC-1	4.B.2.a(14)
SC-5	Denial of Service Protection	10.8.4 13.2.1	---	---	---	6.B.3.a(6)
SC-6	Resource Priority	---	---	---	---	6.B.3.a(11)
SC-7	Boundary Protection	11.4.6	16.2.2 16.2.7 16.2.9 16.2.10 16.2.11 16.2.14	AC-3.2	COEB-1 EBBD-1 ECIM-1 ECVI-1	4.B.4.a(27) 5.B.3.a(11)(b) 7.A.3 7.B 7.C 7.D
SC-8	Transmission Integrity	10.6.1 10.8.1 10.9.1	11.2.1 11.2.4 11.2.9 16.2.14	AC-3.2	ECTM-1	5.B.3.a(11)
SC-9	Transmission Confidentiality	10.6.1 10.8.1 10.9.1	---	---	ECCT-1	4.B.1.a(8)(a)
SC-10	Network Disconnect	11.5.6	16.2.6	AC-3.2	---	4.B.2.a(17)

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
SC-11	Trusted Path	10.9.2	16.2.7	---	---	4.B.4.a(14)
SC-12	Cryptographic Key Establishment and Management	12.3.1 12.3.2	16.1.7 16.1.8	---	IAKM-1	1.G
SC-13	Use of Cryptography	---	16.1.7 16.1.8	---	IAKM-1 IATS-1	1.G.1
SC-14	Public Access Protections	10.7.4 10.9.3	---	---	EBPW-1	---
SC-15	Collaborative Computing	---	---	---	ECVI-1	7.G
SC-16	Transmission of Security Parameters	7.2.2 10.8.2 10.9.2	16.1.6	AC-3.2	ECTM-2	4.B.1.a(3)
SC-17	Public Key Infrastructure Certificates	12.3.2	---	---	IAKM-1	2.B.4.e(5) 4.B.3.a(11)
SC-18	Mobile Code	10.4.1 10.4.2	---	---	DCMC-1	2.B.4.e(5) 7.E
SC-19	Voice Over Internet Protocol	---	---	---	ECVI-1	---[54]
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	---	---	---	---	---
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	---	---	---	---	---
SC-22	Architecture and Provisioning for Name/Address Resolution Service	---	---	---	---	---
SC-23	Session Authenticity	---	---	---	---	---
System and Information Integrity						
SI-1	System and Information Integrity Policy and Procedures	15.1.1	11.	---	DCAR-1	DCID: B.2.a Manual: 2.B.4.e(5) 5.B.1.b(1) 5.B.2.a(5)(a)(1)
SI-2	Flaw Remediation	10.10.5 12.4.1 12.5.1 12.5.2 12.6.1	10.3.2 11.1.1 11.1.2 11.2.2 11.2.7	SS-2.2	DCSQ-1 DCCT-1 VIVM-1	5.B.2.a(5)(a)(3) 6.B.2.a(5)
SI-3	Malicious Code Protection	10.4.1	11.1.1 11.1.2	---	ECVP-1 VIVM-1	5.B.1.a(4) 7.B.4.b(1)
SI-4	Information System Monitoring Tools and Techniques	10.6.2 10.10.1 10.10.2 10.10.4	11.2.5 11.2.6	---	EBBD-1 EBVC-1 ECID-1	4.B.2.a(5)(b) 4.B.3.a(8)(b) 6.B.3.a(8)
SI-5	Security Alerts and Advisories	6.1.7 10.4.1	14.1.1 14.1.2 14.1.5	SP-3.4	VIVM-1	8.B.7
SI-6	Security Functionality Verification	---	11.2.1 11.2.2	SS-2.2	DCSS-1	4.B.1.c(2) 5.B.2.b(2)
SI-7	Software and Information Integrity	12.2.1 12.2.2 12.2.4	11.2.1 11.2.4	---	ECSD-2	4.B.1.c(2) 5.B.1.a(3) 5.B.2.a(6)

[54] Appropriate authorizing officials approve the use of specific technologies, including Voice Over Internet Protocol. See also DCID 6/3 paragraph 2.B.4.d and 9.D.1.a.

CNTL NO.	CONTROL NAME	ISO/IEC 17799	NIST 800-26	GAO FISCAM	DOD 8500.2	DCID 6/3[53]
SI-8	Spam Protection	---	---	---	---	5.B.1.a(4)
SI-9	Information Input Restrictions	12.2.1 12.2.2	---	SD-1	---	2.B.9.b(11)
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	10.7.3 12.2.1 12.2.2	---	---	---	7.B.2.h 2.B.4.d
SI-11	Error Handling	12.2.1 12.2.2 12.2.3 12.2.4	---	---	---	2.B.4.d
SI-12	Information Output Handling and Retention	10.7.3 12.2.4	---	---	PESP-1	2.B.4.d 8.B.9 8.G

APPENDIX H

STANDARDS AND GUIDANCE MAPPINGS

CROSSWALK BETWEEN NIST STANDARDS AND GUIDELINES AND SECURITY CONTROLS

The mapping table in this appendix provides organizations with a two-way crosswalk between NIST security standards and guidance documents (i.e., the current version of the FIPS Publications and Special Publications in the 800- series) and the security controls in the catalog of controls listed in Appendix F. The first crosswalk maps a specific NIST security publication to the associated security controls in NIST Special Publication 800-53 that are relevant to that publication. The second crosswalk maps each security control in Special Publication 800-53 to the appropriate NIST standards and guidance documents that apply to that particular control.[55] The purpose of the crosswalk is to provide organizations with additional useful information regarding security control selection and implementation. The two-way crosswalk between publications and security controls and security controls and publications is not intended to be exhaustive. In addition to providing useful information for organizations, the crosswalk also indicates particular areas where additional security guidance might be needed.

[55] There are certain FIPS and NIST Special Publications that are listed in the crosswalk for a particular security control in Appendix H that do not appear in the supplemental guidance for that control. The supplemental guidance for security controls lists only the most relevant NIST publications associated with that control or the publications that provide the most extensive guidance for that security control area.

CROSSWALK ONE: NIST PUBLICATIONS TO SECURITY CONTROLS

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
FIPS 140-2	Security Requirements for Cryptographic Modules	IA-7, SC-12, SC-13
FIPS 180-2	Secure Hash Standard (SHS)	SC-13
FIPS 186-2	Digital Signature Standard (DSS)	SC-13
FIPS 188	Standard Security Labels for Information Transfer	AC-16
FIPS 190	Guideline for the Use of Advanced Authentication Technology Alternatives	IA-1, IA-5, SC-13
FIPS 197	Advanced Encryption Standard, November 2001	SC-13
FIPS 198	The Keyed-Hash Message Authentication Code (HMAC)	AU-10, SC-8, SC-13
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems	PL-2, RA-2
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PS-1, RA-1, SA-1, SC-1, SI-1
FIPS 201-1	Personal Identity Verification (PIV) of Federal Employees and Contractors	AC-1, AC-3, AC-17, IA-1, IA-2, IA-4, IA-5, PL-5, SC-13, SC-17
SP 800-12	An Introduction to Computer Security: The NIST Handbook	AC-1, AC-2, AC-3, AC-6, AC-13, AC-16, AT-1, AU-1, AU-2, AU-3, AU-6, AU-7, AU-9, CA-1, CM-1, CP-1, CP-2, CP-4, IA-1, IA-2, IR-1, MA-1, MP-1, PE-1, PE-3, PE-4, PE-13, PL-1, PL-2, PL-5, PS-1, PS-2, PS-3, PS-4, PS-5, RA-1, RA-3, RA-4, SA-1, SA-3, SC-1, SC-12, SC-13, SC-14, SI-1
SP 800-13	Telecommunications Security Guidelines for Telecommunications Management Network	CP-8, RA-3, RA-4
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, CP-2, CP-5, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PL-2, PS-1, PS-4, RA-1, RA-3, RA-4, SA-1, SA-3, SC-1, SI-1
SP 800-15	Minimum Interoperability Specification for PKI Components (MISPC), Version 1	SC-17
SP 800-16	Information Technology Security Training Requirements: A Role- and Performance-Based Model	AT-3
SP 800-17	Modes of Operation Validation System (MOVS): Requirements and Procedures	CA-2, SC-13
SP 800-18	Guide for Developing Security Plans for Federal Information Systems	CA-3, CA-5, PL-1, PL-2, PL-3
SP 800-19	Mobile Agent Security	AC-1, AC-3, AC-6, AU-3, AU-9, PL-2, PL-5, RA-3, RA-4, SC-2, SI-3, SI-7
SP 800-20	Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures	CA-2, SC-13

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-21-1	Second Edition, Guideline for Implementing Cryptography in the Federal Government	CP-9, CP-10, PL-2, SA-3, SC-12, SC-13
SP 800-22	A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications	CA-2, SC-13
SP 800-23	Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products	CA-1, CA-2, RA-3, RA-4, SA-4
SP 800-24	PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does	AC-17, CP-10, IA-2, MA-2, MP-6, PE-3, RA-3, RA-4, RA-5
SP 800-25	Federal Agency Use of Public Key Technology for Digital Signatures and Authentication	CP-9, IA-1, IA-5, PL-2, RA-3, RA-4, SC-17
SP 800-27	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)	PL-2, SA-3, SA-8
SP 800-28	Guidelines on Active Content and Mobile Code	AC-6, RA-3, RA-4, SC-1, SC-7, SC-15, SC-18, SI-2
SP 800-29	A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2	SC-13
SP 800-30	Risk Management Guide for Information Technology Systems	CA-5, PL-2, RA-1, RA-2, RA-3, RA-4, SA-3
SP 800-32	Introduction to Public Key Technology and the Federal PKI Infrastructure	IA-5, PL-2, RA-3, RA-4, SC-17, SC-20
SP 800-33	Underlying Technical Models for Information Technology Security	PL-2, SA-8
SP 800-34	Contingency Planning Guide for Information Technology Systems	CP-1, CP-2, CP-3, CP-4, CP-5, CP-6, CP-7, CP-8, CP-9, CP-10, MA-1, PL-2, RA-3, RA-4, SA-3
SP 800-35	Guide to Information Technology Security Services	CA-2, CM-2, CM-8, SA-1, SA-2, SA-3, SA-9
SP 800-36	Guide to Selecting Information Technology Security Products	AC-1, CA-2, IA-1, IR-4, MP-6, RA-5, SA-1, SA-4, SC-7, SC-17, SI-3, SI-4
SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems	CA-1, CA-2, CA-4, CA-5, CA-6, CA-7, CM-1, PL-2, PL-3, RA-1, RA-2, RA-3, RA-4, RA-5
SP 800-38A	Recommendation for Block Cipher Modes of Operation - Methods and Techniques	SC-13
SP 800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication	SC-13
SP 800-38C	Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality	SC-13
SP 800-38D	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication (Draft)	SC-13

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-39	Managing Risk from Information Systems: An Organizational Perspective (Draft)	CA-5, PL-2, RA-1, RA-2, RA-3, RA-4, SA-3
SP 800-40	Creating a Patch and Vulnerability Management Program	AT-3, AT-5, CM-2, CM-6, CM-8, PL-2, RA-2, RA-3, RA-4, RA-5, SI-2, SI-4, SI-5
SP 800-41	Guidelines on Firewalls and Firewall Policy	AC-1, AC-4, CP-9, PL-2, SC-7
SP 800-42	Guideline on Network Security Testing	AU-6, CA-7, PL-1, RA-3, RA-4, RA-5, SI-3, SI-4
SP 800-43	Systems Administration Guidance for Windows 2000 Professional	AC-2, CM-6, SI-2, CP-9, CP-10
SP 800-44	Guidelines on Securing Public Web Servers	AC-1, AC-17, AU-1, AU-2, AU-6, AU-7, IA-2, CM-6, CP-9, CP-10, IA-1, PL-2, PL-5, RA-3, RA-4, RA-5, SC-5, SC-7, SC-8, SC-9, SI-4, SI-7, SI-10
SP 800-45	Guidelines on Electronic Mail Security	AC-1, AC-17, AU-2, AU-6, AU-9, CM-6, CP-9, IA-1, PL-2. PL-4, RA-3, RA-4, RA-5, SC-8, SC-9, SI-3, SI-8
SP 800-46	Security for Telecommuting and Broadband Communications	AC-1, AC-17, AC-18, AC-20, CM-6. IA-1, IA-2, PL-4, RA-3, RA-4, RA-5, SC-7, SC-10
SP 800-47	Security Guide for Interconnecting Information Technology Systems	CA-3
SP 800-48	Wireless Network Security: 802.11, Bluetooth, and Handheld Devices	AC-18, CM-6, IA-3, PL-4, RA-3, RA-4, SI-4
SP 800-49	Federal S/MIME V3 Client Profile	AU-10, SC-8, SC-9
SP 800-50	Building an Information Technology Security Awareness and Training Program	AT-1, AT-2, AT-3, AT-4, CP-3, IR2
SP 800-51	Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme	RA-5, SI-2, SI-5
SP 800-52	Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations	AU-10, IA-3, SC-8, SC-9, SC-12, SC-23
SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems (Draft)	CA-2, CA-4, CA-7
SP 800-54	Border Gateway Protocol Security	CM-6, RA-3, RA-4, SC-5, SC-7, SC-8, SC-9, SC-23
SP 800-55	Security Metrics Guide for Information Technology Systems	CA-1, CA-2, CA-4, CA-7, RA-3, RA-4
SP 800-56A	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography	CP-4, SC-12, SC-17
SP 800-57	Recommendation on Key Management	AC-16, AU-1, CP-9, CP-10, MP-5, PL-2, SC-8, SC-9, SC-12, SC-17, SI-7, SI-10
SP 800-58	Security Considerations for Voice Over IP Systems	AC-4, AC-17, AC-18, IA-3, PE-4, PE-11, PL-2, SC-7, SC-8, SC-9, SC-12, SC-16, SC-19
SP 800-59	Guideline for Identifying an Information System as a National Security System	RA-2

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-60	Guide for Mapping Types of Information and Information Systems to Security Categories	RA-2, RA-3, RA-4
SP 800-61	Computer Security Incident Handling Guide	IR-1, IR-2, IR-3, IR-4, IR-5, IR-6, IR-7, SI-5
SP 800-63	Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology	IA-1, IA-5, RA-3, RA-4
SP 800-64	Security Considerations in the Information System Development Life Cycle	PL-2, SA-1, SA-2, SA-3, SA-4
SP 800-65	Integrating Security into the Capital Planning and Investment Control Process	CA-5, PL-1, RA-3, RA-4, SA-1, SA-2
SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	AC-1, AC-2, AC-3, AC-5, AC-6, AT-1, AT-2, AT-3, AU-1, AU-2, CA-1, CA-2, CA-3, CA-4, CA-6, CP-1, CP-2, CP-4, IA-4, IA-5, IR-1, MP-1, MP-4, MP-6, PE-1, PE-3, PE-18, PL-1, PS-1, PS-4, PS-8, RA-1, RA-2, RA-3, RA-4, SA-1, SA-9, SC-8, SC-9, SI-1, SI-7
SP 800-67	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher	SC-13
SP 800-68	Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist	AC-3, AC-6, AC-7, AC-17, AU-2, AU-4, CM-6, IA-2, IA-5, SC-5
SP 800-69	Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist	AC-6, CP-9, IA-2, SI-3
SP 800-70	Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers	CM-6, SC-7
SP 800-72	Guidelines on PDA Forensics	AU-1, AU-2, AU-9, IA-3, IA-4, IA-6, MP-1, MP-2, MP-5
SP 800-73	Interfaces for Personal Identity Verification	AC-3, AC-17, IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, PE-3, SC-12
SP 800-76-1	Biometric Data Specification for Personal Identity Verification	AC-3, AC-17, CA-2, CA-4, IA-1, IA-2, IA-5, PE-3, SA-11
SP 800-77	Guide to IPsec VPNs	AC-4, AC-17, AC-20, IA-3, IA-5, MA-4, SC-7, SC-8, SC-9, SC-12, SC-23
SP 800-78-1	Cryptographic Algorithms and Key Sizes for Personal Identity Verification	AC-3, AC-17, IA-2, IA-4, IA-5, IA-7, PE-3, SC-13
SP 800-79	Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations	CA-1, CA-2, CA-4, CA-6, CA-7
SP 800-81	Secure Domain Name System (DNS) Deployment Guide	AC-6, CM-6, CM-7, CP-10, IA-3, PL-2, SC-3, SC-5, SC-8, SC-20, SC-21, SC-22
SP 800-82	Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security (Draft)	AC-4, CM-6, CP-2, PE-3, RA-3, RA-4, RA-5, SC-7

PUBLICATION NO.	PUBLICATION TITLE	RELATED SECURITY CONTROLS
SP 800-83	Guide to Malware Incident Prevention and Handling	AC-6, AU-2, AU-5, AU-6, CM-4, CM-6, CM-7, CP-10, IR-1, IR-4, RA-5, SA-7, SC-7, SI-2, SI-3, SI-4
SP 800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	CP-1, CP-3, CP-4, IR-1, IR-2, IR-3
SP 800-85A	PIV Card Application and Middleware Interface Test Guidelines	CA-4, CA-7, SA-11, SI-6
SP 800-85B	PIV Data Model Test Guidelines	CA-4, CA-7, SA-11, SI-6
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response	IR-1, IR-4
SP 800-87	Codes for the Identification of Federal and Federally-Assisted Organizations	AC-3, AC-17, IA-1, IA-2, IA-4, IA-5, IA-7
SP 800-88	Guidelines for Media Sanitization	MA-1, MP-1, MP-4, MP-6
SP 800-89	Recommendation for Obtaining Assurances for Digital Signature Applications	AU-10, PL-4, SC-17
SP 800-90	Recommendation for Random Number Generation Using Deterministic Random Bit Generators	SC-13
SP 800-92	Guide to Computer Security Log Management, September 2006	AU-1, AU-2, AU-3, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, IR-4, MP-4, MP-5, SI-4
SP 800-94	Guide to Intrusion Detection and Prevention (IDP) Systems	AU-2, AU-3, AU-6, AU-8, AU-9, IR-4, PL-2, RA-3, RA-4, RA-5, SA-4, SC-5, SI-1, SI-3, SI-4, SI-7
SP 800-95	Guide to Secure Web Services	AC-3, AU-10, SC-5, SC-8, SC-9, SC-23
SP 800-96	PIV Card / Reader Interoperability Guidelines	AC-3, AC-17, IA-2, IA-3, IA-4, IA-5, PE-3
SP 800-97	Guide to IEEE 802.11i: Establishing Robust Security Networks	AC-18, IA-2, IA-3, SC-8, SC-9, SC-12, SA-3
SP 800-98	Guidance for Securing Radio Frequency Identification (RFID) Systems	AC-3, AC-5, CP-10, MP-6, PE-3, PE-19, PL-5, RA-3, RA-4, SA-3
SP 800-100	Information Security Handbook: A Guide for Managers	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1
SP 800-101	Guidelines on Cell Phone Forensics	IR-4

CROSSWALK TWO: SECURITY CONTROLS TO NIST PUBLICATIONS

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
Access Control		
AC-1	Access Control Policy and Procedures	FIPS 200, 201-1; NIST Special Publications 800-12, 800-14, 800-19, 800-36, 800-41, 800-44, 800-45, 800-46, 800-66, 800-100
AC-2	Account Management	NIST Special Publications 800-12, 800-43, 800-66
AC-3	Access Enforcement	FIPS 201-1; NIST Special Publications 800-12, 800-19, 800-66, 800-68, 800-73, 800-76, 800-78, 800-87, 800-95, 800-96, 800-98
AC-4	Information Flow Enforcement	NIST Special Publications 800-41, 800-77, 800-82
AC-5	Separation of Duties	NIST Special Publication 800-66, 800-98
AC-6	Least Privilege	NIST Special Publications 800-12, 800-19, 800-28 800-66, 800-68, 800-69, 800-81, 800-83
AC-7	Unsuccessful Login Attempts	NIST Special Publication 800-68
AC-8	System Use Notification	No references available.
AC-9	Previous Logon Notification	No references available.
AC-10	Concurrent Session Control	No references available.
AC-11	Session Lock	No references available.
AC-12	Session Termination	No references available.
AC-13	Supervision and Review—Access Control	NIST Special Publication 800-12
AC-14	Permitted Actions without Identification or Authentication	No references available.
AC-15	Automated Marking	No references available.
AC-16	Automated Labeling	FIPS 188; NIST Special Publications 800-12, 800-57
AC-17	Remote Access	FIPS 201-1; NIST Special Publications 800-24, 800-44, 800-45, 800-46, 800-58, 800-68, 800-73, 800-76. 800-77, 800-78, 800-87, 800-96
AC-18	Wireless Access Restrictions	NIST Special Publications 800-46, 800-48, 800-58, 800-97
AC-19	Access Control for Portable and Mobile Systems	No references available.
AC-20	Use of External Information Systems	NIST Special Publications 800-46, 800-77
Awareness and Training		
AT-1	Security Awareness and Training Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-50, 800-66, 800-100
AT-2	Security Awareness	NIST Special Publications 800-50, 800-66
AT-3	Security Training	NIST Special Publications 800-16, 800-40, 800-50, 800-66
AT-4	Security Training Records	NIST Special Publications 800-50
AT-5	Contacts with Security Groups and Associations	NIST Special Publications 800-40
Audit and Accountability		
AU-1	Audit and Accountability Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-44, 800-57, 800-66, 800-72, 800-92, 800-100

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
AU-2	Auditable Events	NIST Special Publications 800-12, 800-44, 800-45, 800-66, 800-68, 800-72, 800-83, 800-92, 800-94
AU-3	Content of Audit Records	NIST Special Publications 800-12, 800-19, 800-92, 800-94
AU-4	Audit Storage Capacity	NIST Special Publications 800-68, 800-92
AU-5	Response to Audit Processing Failures	NIST Special Publications 800-83, 800-92
AU-6	Audit Monitoring, Analysis, and Reporting	NIST Special Publications 800-12, 800-42, 800-44, 800-45, 800-83, 800-92, 800-94
AU-7	Audit Reduction and Report Generation	NIST Special Publications 800-12, 800-44, 800-92
AU-8	Time Stamps	NIST Special Publications 800-92, 800-94
AU-9	Protection of Audit Information	NIST Special Publications 800-12, 800-19, 800-45, 800-72, 800-92, 800-94
AU-10	Non-repudiation	FIPS 198; NIST Special Publications 800-49, 800-52, 800-89, 800-95
AU-11	Audit Record Retention	NIST Special Publication 800-92
Certification, Accreditation, and Security Assessments		
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-23, 800-37, 800-53A, 800-66, 800-79, 800-100
CA-2	Security Assessments	NIST Special Publications 800-17, 800-20, 800-22, 800-23, 800-35, 800-36, 800-37, 800-53A, 800-55, 800-66, 800-76, 800-79
CA-3	Information System Connections	NIST Special Publications 800-18, 800-47, 800-66
CA-4	Security Certification	NIST Special Publications 800-37, 800-53A, 800-66, 800-76, 800-79, 800-85A, 800-85B
CA-5	Plan of Action and Milestones	NIST Special Publications 800-18, 800-30, 800-37, 800-65
CA-6	Security Accreditation	NIST Special Publications 800-37, 800-66, 800-79
CA-7	Continuous Monitoring	NIST Special Publications 800-37, 800-42, 800-53A, 800-79 800-85A, 800-85B
Configuration Management		
CM-1	Configuration Management Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-37, 800-100
CM-2	Baseline Configuration	NIST Special Publications 800-35, 800-40, 800-82
CM-3	Configuration Change Control	No references available.
CM-4	Monitoring Configuration Changes	NIST Special Publication 800-83
CM-5	Access Restrictions for Change	No references available.
CM-6	Configuration Settings	NIST Special Publications 800-40, 800-43, 800-44, 800-45, 800-46, 800-48, 800-54, 800-68, 800-70, 800-81, 800-82, 800-83
CM-7	Least Functionality	NIST Special Publications 800-81, 800-83
CM-8	Information System Component Inventory	NIST Special Publications 800-35, 800-40
Contingency Planning		
CP-1	Contingency Planning Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-34, 800-66, 800-84, 800-100

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
CP-2	Contingency Plan	NIST Special Publications 800-12, 800-14, 800-34, 800-66
CP-3	Contingency Training	NIST Special Publications 800-34, 800-50, 800-84
CP-4	Contingency Plan Testing	NIST Special Publications 800-12, 800-34, 800-56, 800-66, 800-84
CP-5	Contingency Plan Update	NIST Special Publications 800-14, 800-34
CP-6	Alternate Storage Site	NIST Special Publication 800-34
CP-7	Alternate Processing Site	NIST Special Publication 800-34
CP-8	Telecommunications Services	NIST Special Publications 800-13, 800-34
CP-9	Information System Backup	NIST Special Publications 800-21, 800-25, 800-34, 800-41, 800-43, 800-44, 800-45, 800-57, 800-69
CP-10	Information System Recovery and Reconstitution	NIST Special Publications 800-21, 800-24, 800-34, 800-43, 800-44, 800-57, 800-81, 800-83, 800-98
Identification and Authentication		
IA-1	Identification and Authentication Policy and Procedures	FIPS 190, FIPS 200, FIPS 201-1; NIST Special Publications 800-12, 800-14, 800-25, 800-36, 800-44, 800-45, 800-46, 800-63, 800-73, 800-76, 800-87, 800-100
IA-2	User Identification and Authentication	FIPS 201-1; NIST Special Publications 800-12, 800-24, 800-44, 800-46, 800-68, 800-69, 800-73, 800-76, 800-78, 800-87, 800-96, 800-97
IA-3	Device Identification and Authentication	NIST Special Publications 800-48, 800-52, 800-72, 800-73, 800-77, 800-81, 800-96, 800-97
IA-4	Identifier Management	FIPS 201-1; NIST Special Publications 800-66, 800-72, 800-73, 800-78, 800-87, 800-96
IA-5	Authenticator Management	FIPS 190, 201-1; NIST Special Publications 800-25, 800-32, 800-63, 800-66, 800-68, 800-73, 800-76, 800-77, 800-78, 800-87, 800-96
IA-6	Authenticator Feedback	NIST Special Publication 800-72
IA-7	Cryptographic Module Authentication	FIPS 140-2; NIST Special Publications 800-73, 800-78, 800-87
Incident Response		
IR-1	Incident Response Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-61, 800-66, 800-86, 800-83, 800-84, 800-100
IR-2	Incident Response Training	NIST Special Publications 800-50, 800-61, 800-84
IR-3	Incident Response Testing	NIST Special Publication 800-61, 800-84
IR-4	Incident Handling	NIST Special Publications 800-36, 800-61, 800-83, 800-86, 800-92, 800-94, 800-101
IR-5	Incident Monitoring	NIST Special Publication 800-61
IR-6	Incident Reporting	NIST Special Publication 800-61
IR-7	Incident Response Assistance	NIST Special Publication 800-61
Maintenance		
MA-1	System Maintenance Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-34, 800-88, 800-100
MA-2	Controlled Maintenance	NIST Special Publication 800-24
MA-3	Maintenance Tools	No references available.
MA-4	Remote Maintenance	NIST Special Publication 800-77

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
MA-5	Maintenance Personnel	No references available.
MA-6	Timely Maintenance	No references available.
Media Protection		
MP-1	Media Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-72, 800-88, 800-100
MP-2	Media Access	NIST Special Publication 800-72
MP-3	Media Labeling	No references available.
MP-4	Media Storage	NIST Special Publications 800-66, 800-88, 800-92
MP-5	Media Transport	NIST Special Publications 800-57, 800-72, 800-92
MP-6	Media Sanitization and Disposal	NIST Special Publications 800-24, 800-36, 800-66, 800-88, 800-98
Physical and Environmental Protection		
PE-1	Physical and Environmental Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100
PE-2	Physical Access Authorizations	No references available.
PE-3	Physical Access Control	NIST Special Publications 800-12, 800-24, 800-66, 800-73, 800-76, 800-78, 800-82, 800-96, 800-98
PE-4	Access Control for Transmission Medium	NIST Special Publications 800-12, 800-58
PE-5	Access Control for Display Medium	No references available.
PE-6	Monitoring Physical Access	No references available.
PE-7	Visitor Control	No references available.
PE-8	Access Records	No references available.
PE-9	Power Equipment and Power Cabling	No references available.
PE-10	Emergency Shutoff	No references available.
PE-11	Emergency Power	NIST Special Publication 800-58
PE-12	Emergency Lighting	No references available.
PE-13	Fire Protection	NIST Special Publication 800-12
PE-14	Temperature and Humidity Controls	No references available.
PE-15	Water Damage Protection	No references available.
PE-16	Delivery and Removal	No references available.
PE-17	Alternate Work Site	No references available.
PE-18	Location of Information System Components	NIST Special Publication 800-66
PE-19	Information Leakage	NIST Special Publication 800-98
Planning		
PL-1	Security Planning Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-18, 800-42, 800-65, 800-66, 800-100
PL-2	System Security Plan	FIPS 199, 200; NIST Special Publications 800-12, 800-14, 800-18, 800-19, 800-21, 800-25, 800-27, 800-30, 800-32, 800-33, 800-34, 800-37, 800-40, 800-41, 800-44, 800-45, 800-57, 800-58, 800-64, 800-81
PL-3	System Security Plan Update	NIST Special Publications 800-18, 800-37

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
PL-4	Rules of Behavior	NIST Special Publications 800-45, 800-46, 800-48, 800-89
PL-5	Privacy Impact Assessment	FIPS 201-1; NIST Special Publications 800-12, 800-19, 800-44, 800-98
PL-6	Security-Related Activity Planning	No references available.
Personnel Security		
PS-1	Personnel Security Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-100
PS-2	Position Categorization	NIST Special Publication 800-12
PS-3	Personnel Screening	NIST Special Publication 800-12
PS-4	Personnel Termination	NIST Special Publications 800-12, 800-14, 800-66
PS-5	Personnel Transfer	NIST Special Publication 800-12
PS-6	Access Agreements	No references available.
PS-7	Third-Party Personnel Security	No references available.
PS-8	Personnel Sanctions	NIST Special Publication 800-66
Risk Assessment		
RA-1	Risk Assessment Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-30, 800-37, 800-66, 800-100
RA-2	Security Categorization	FIPS 199; NIST Special Publications 800-30, 800-37, 800-40, 800-59, 800-60, 800-66
RA-3	Risk Assessment	NIST Special Publications 800-12, 800-13, 800-14, 800-19, 800-23, 800-24, 800-25, 800-28, 800-30, 800-32, 800-34, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-48, 800-53A, 800-54, 800-60, 800-63, 800-65, 800-66, 800-82, 800-94, 800-98
RA-4	Risk Assessment Update	NIST Special Publications 800-12, 800-13, 800-14, 800-19, 800-23, 800-24, 800-25, 800-28, 800-30, 800-32, 800-34, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-48, 800-53A, 800-54, 800-60, 800-63, 800-65, 800-66, 800-82, 800-94, 800-98
RA-5	Vulnerability Scanning	NIST Special Publications 800-24, 800-36, 800-37, 800-40, 800-42, 800-44, 800-45, 800-46, 800-51, 800-83, 800-94
System and Services Acquisition		
SA-1	System and Services Acquisition Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-35, 800-36, 800-64, 800-65, 800-66, 800-100
SA-2	Allocation of Resources	NIST Special Publications 800-35, 800-64, 800-65
SA-3	Life Cycle Support	NIST Special Publications 800-12, 800-14, 800-21, 800-27, 800-30, 800-34, 800-35, 800-64, 800-97, 800-98
SA-4	Acquisitions	NIST Special Publications 800-23, 800-36, 800-64, 800-94
SA-5	Information System Documentation	No references available.
SA-6	Software Usage Restrictions	No references available.
SA-7	User Installed Software	NIST Special Publication 800-83
SA-8	Security Engineering Principles	NIST Special Publications 800-27, 800-33
SA-9	External Information System Services	NIST Special Publications 800-35, 800-66
SA-10	Developer Configuration Management	No references available.
SA-11	Developer Security Testing	NIST Special Publications 800-76, 800-85A, 800-85B
System and Communications Protection		

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
SC-1	System and Communications Protection Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-28, 800-100
SC-2	Application Partitioning	NIST Special Publication 800-19
SC-3	Security Function Isolation	NIST Special Publication 800-81
SC-4	Information Remnance	No references available.
SC-5	Denial of Service Protection	NIST Special Publications 800-44, 800-54, 800-68, 800-81, 800-94, 800-95
SC-6	Resource Priority	No references available.
SC-7	Boundary Protection	NIST Special Publications 800-28, 800-36, 800-41, 800-44, 800-46, 800-54, 800-58, 800-70, 800-77, 800-82, 800-83
SC-8	Transmission Integrity	FIPS 198; NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-57, 800-54, 800-58, 800-66, 800-77, 800-81, 800-95, 800-97
SC-9	Transmission Confidentiality	NIST Special Publications 800-44, 800-45, 800-49, 800-52, 800-54, 800-57, 800-58, 800-66, 800-77, 800-95, 800-97
SC-10	Network Disconnect	NIST Special Publication 800-46
SC-11	Trusted Path	No references available.
SC-12	Cryptographic Key Establishment and Management	FIPS 140-2; NIST Special Publications 800-12, 800-21, 800-52, 800-56, 800-57, 800-58, 800-73, 800-77, 800-97
SC-13	Use of Cryptography	FIPS 140-2, 180-2, 186-2, 190, 197 198, 201-1; NIST Special Publications 800-12, 800-17, 800-20, 800-21, 800-22, 800-29, 800-38A, 800-38B, 800-38C, 800-38D, 800-67, 800-78, 800-90
SC-14	Public Access Protections	NIST Special Publication 800-12
SC-15	Collaborative Computing	No references available.
SC-16	Transmission of Security Parameters	No references available.
SC-17	Public Key Infrastructure Certificates	FIPS 201; NIST Special Publications 800-15, 800-25, 800-32, 800-36, 800-56, 800-57, 800-89
SC-18	Mobile Code	NIST Special Publication 800-28
SC-19	Voice Over Internet Protocol	NIST Special Publication 800-58
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	NIST Special Publications 800-32, 800-81
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	NIST Special Publication 800-81
SC-22	Architecture and Provisioning for Name/Address Resolution Service	NIST Special Publication 800-81
SC-23	Session Authenticity	NIST Special Publications 800-52, 800-54, 800-77, 800-95
System and Information Integrity		
SI-1	System and Information Integrity Policy and Procedures	FIPS 200; NIST Special Publications 800-12, 800-14, 800-66, 800-94, 800-100
SI-2	Flaw Remediation	NIST Special Publications 800-28, 800-40, 800-43, 800-51, 800-83
SI-3	Malicious Code Protection	NIST Special Publications 800-19, 800-36, 800-42, 800-45, 800-69, 800-83, 800-94
SI-4	Information System Monitoring Tools and Techniques	NIST Special Publications 800-36, 800-40, 800-42, 800-44 800-48, 800-83, 800-92, 800-94
SI-5	Security Alerts and Advisories	NIST Special Publications 800-40, 800-51, 800-61

CNTL NO.	CONTROL NAME	RELATED NIST PUBLICATIONS
SI-6	Security Functionality Verification	NIST Special Publication 800-85A, 800-85B
SI-7	Software and Information Integrity	NIST Special Publications 800-19, 800-44, 800-57, 800-66, 800-94
SI-8	Spam Protection	NIST Special Publication 800-45
SI-9	Information Input Restrictions	No references available.
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	NIST Special Publications 800-44, 800-57
SI-11	Error Handling	No references available.
SI-12	Information Output Handling and Retention	No references available.

APPENDIX I

INDUSTRIAL CONTROL SYSTEMS

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

Industrial control systems (ICS)[56] are information systems that differ significantly from traditional administrative, mission support, and scientific data processing information systems. ICS typically have many unique characteristics—including a need for real-time response and extremely high availability, predictability, and reliability. These types of specialized systems are pervasive throughout the critical infrastructure, often being required to meet several and often conflicting safety, operational, performance, reliability, and security requirements such as: (i) minimizing risk to the health and safety of the public; (ii) preventing serious damage to the environment; (iii) preventing serious production stoppages or slowdowns that result in negative impact to the Nation's economy and ability to carry out critical functions; (iv) protecting the critical infrastructure from cyber attacks and common human error; and (v) safeguarding against the compromise of proprietary information.[57]

Until recently, ICS had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. Increasingly, ICS use the same commercially available hardware and software components as are used in the organization's traditional information systems. While the change in industrial control system architecture supports new information system capabilities, it also provides significantly less isolation from the outside world for these systems, introducing many of the same vulnerabilities that exist in current networked information systems. The result is an even greater need to secure ICS.

FIPS 200, in combination with NIST Special Publication 800-53, requires that federal agencies implement minimum security controls for their organizational information systems based on the FIPS 199 security categorization of those systems. This includes implementing the minimum baseline security controls described in NIST Special Publication 800-53 in ICS that are operated by or on behalf of federal agencies. Section 3.3, *Tailoring the Initial Baseline,* allows the organization[58] to modify or adjust the recommended security control baselines when certain conditions exist that require that flexibility. NIST recommends that ICS owners take advantage of the ability to tailor the initial baselines applying the ICS-specific guidance in this appendix. This appendix also contains additions to the initial baselines that have been determined to be generally required for ICS.

[56] An ICS is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC). ICS are typically found in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries as well as in air and rail transportation control systems.

[57] See Executive Order 13231 on Critical Infrastructure Protection, October 16, 2001.

[58] NIST Special Publication 800-53 employs the term *organization* to refer to the owner or operator of an information system. In this Appendix, organization may refer to the owner or operator of an ICS.

NIST has worked cooperatively with ICS communities in the public and private sectors to develop specific guidance on the application of the security controls in Special Publication 800-53 to ICS. That guidance, contained in this Appendix, includes ICS-specific:

- Tailoring guidance;
- Security control enhancements;
- Supplements to the security control baselines; and
- Supplemental guidance.

ICS Tailoring Guidance

Tailoring guidance for ICS can include scoping guidance and the application of compensating security controls. Due to the unique characteristics of ICS, these systems may require a greater use of compensating security controls than is the case for general purpose information systems.

In situations where the ICS cannot support, or the organization determines it is not advisable to implement particular security controls or control enhancements in an ICS (e.g., performance, safety, or reliability are adversely impacted), the organization provides a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the ICS and why the related baseline security controls could not be employed.

If the ICS cannot support the use of automated mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance in Section 3.3.

Compensating controls are not exceptions or waivers to the baseline controls; rather, they are alternative safeguards and countermeasures employed within the ICS that accomplish the intent of the original security controls that could not be effectively employed. Organizational decisions on the use of compensating controls are documented in the security plan for the ICS.

The security controls and control enhancements listed in Table I-1 are likely candidates for tailoring (i.e., requiring the application of scoping guidance and/or compensating controls) with regard to ICS. Note that the parenthetical numbers following the control identification refer to control enhancements.

TABLE I-1: SECURITY CONTROL CANDIDATES FOR TAILORING

CONTROL NO.	CONTROL NAME	TAILORING OPTIONS	
		SCOPING GUIDANCE	COMPENSATING CONTROLS
AC-2	Account Management	NO	YES
AC-2 (1)	Account Management	YES	YES
AC-5	Separation of Duties	NO	YES
AC-6	Least Privilege	NO	YES
AC-7	Unsuccessful Login Attempts	NO	YES
AC-8	System Use Notification	NO	YES
AC-10	Concurrent Session Control	NO	YES
AC-11	Session Lock	NO	YES

CONTROL NO.	CONTROL NAME	TAILORING OPTIONS	
		SCOPING GUIDANCE	COMPENSATING CONTROLS
AC-12	Session Termination	YES	YES
AC-13 (1)	Supervision and Review – Access Control	YES	YES
AC-15	Automated Marking	YES	YES
AC-16	Automated Labeling	YES	YES
AC-17 (1)	Remote Access	YES	YES
AC-17 (2)	Remote Access	NO	YES
AC-18 (1)	Wireless Access Restrictions	NO	YES
AU-2	Auditable Events	NO	YES
AU-6	Audit Monitoring, Analysis, and Reporting	NO	YES
AU-7	Audit Reduction and Report Generation	NO	YES
CA-2	Security Assessments	NO	YES
CA-4	Security Certification	NO	YES
CM-3 (1)	Configuration Change Control	YES	YES
CM-3 (ICS-1)	Configuration Change Control	NO	YES
CM-5 (1)	Access Restrictions for Change	YES	YES
CM-6 (1)	Configuration Settings	YES	YES
CP-4	Contingency Plan Testing and Exercises	NO	YES
CP-7	Alternate Processing Site	NO	YES
IA-2	User Identification and Authentication	NO	YES
IA-3	Device Identification and Authentication	NO	YES
MA-3 (4)	Maintenance Tools	YES	YES
MA-4 (3)	Remote Maintenance	YES	YES
PE-6 (2)	Monitoring Physical Access	YES	YES
RA-5	Vulnerability Scanning	NO	YES
SC-3	Security Function Isolation	NO	YES
SC-10	Network Disconnect	NO	YES
SI-2 (1)	Flaw Remediation	YES	YES
SI-2 (2)	Flaw Remediation	YES	YES
SI-3 (1)	Malicious Code Protection	YES	YES
SI-3 (2)	Malicious Code Protection	YES	YES
SI-6 (2)	Security Functionality Verification	YES	YES
SI-8 (1)	Spam Protection	YES	YES
SI-8 (2)	Spam Protection	YES	YES

ICS Security Control Enhancements

ICS security control enhancements are augmentations to the original controls in Appendix F that are required for certain ICS. The following ICS control enhancements extend the security control catalog in Appendix F:

AC-3 ACCESS ENFORCEMENT

ICS Control Enhancements:

(ICS-1) The ICS requires dual authorization, based on approved organizational procedures, to privileged functions that have impacts on facility, public, and environmental safety.

ICS Enhancement Supplemental Guidance: The organization does not employ dual-approval mechanisms when an immediate response is necessary to ensure public and environmental safety.

CM-3 CONFIGURATION CHANGE CONTROL

ICS Control Enhancements:

(ICS-1) The organization tests, validates, and documents changes (e.g., patches and updates) before implementing the changes on the operational ICS.

ICS Enhancement Supplemental Guidance: The organization ensures that testing does not interfere with ICS functions. The individual/group conducting the tests fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an ICS must be taken off-line for testing, the tests are scheduled to occur during planned ICS outages whenever possible. In situations where the organization cannot, for operational reasons, conduct live testing of a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

ICS Supplements to the Security Control Baselines

The following table lists the recommended ICS supplements (highlighted in **bold** text) to the security controls baselines in Appendix D.

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-3	Access Enforcement	AC-3	AC-3 (1) **(ICS-1)**	AC-3 (1) **(ICS-1)**
Configuration Management				
CM-3	Configuration Change Control	Not Selected	CM-3 **(ICS-1)**	CM-3 (1) **(ICS-1)**
Physical and Environmental Protection				
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9 **(1)**	PE-9 **(1)**
PE-11	Emergency Power	**PE-11**	PE-11 **(1)**	PE-11 (1) **(2)**

In addition to the enhancements added for ICS in the table above, the security control supplement process described in Section 3.4 is still applicable to ICS. Organizations are required to conduct a risk assessment taking into account the tailoring and supplementing performed in arriving at the agreed upon set of security controls for the ICS and the risk to the organization's operations and assets, individuals, other organizations, and the Nation being incurred by operation of the ICS with the intended controls. The organization decides whether that risk is acceptable, and if not, supplements the control set with additional controls until an acceptable level of risk is obtained.

ICS Supplemental Guidance

ICS Supplemental Guidance provides organizations with additional information on the application of the security controls and control enhancements in Appendix F to ICS and the environments in which these specialized systems operate. The Supplemental Guidance also provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls). ICS Supplemental Guidance does not replace the original Supplemental Guidance in Appendix F.[59]

ACCESS CONTROL

AC-2 ACCOUNT MANAGEMENT

ICS Supplemental Guidance: Account management may include additional account types (e.g., role-based, device-based, attribute-based). The organization removes, disables, or otherwise secures default accounts (e.g., accounts used for maintenance) and changes default passwords. In situations where physical access to the ICS (e.g., workstations, hardware components, or field devices) predefines account privileges or where the ICS (e.g., certain remote terminal units, meters, or relays) cannot support account management, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, intrusion detection, and auditing measures) in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support the use of automated mechanisms for the management of information system accounts, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-3 ACCESS ENFORCEMENT

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS. NIST Special Publication 800-82 provides guidance on ICS access enforcement.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: Within ICS, it is commonly the case that having access to specific devices (e.g., workstations, remote terminal units, field devices) is the equivalent to having privileged access; thereby restricting access to these devices is also restricting access to privileged functions and security-relevant information.

[59] In certain cases, the ICS-specific Supplemental Guidance developed during the ICS Security Project has applicability to general purpose information systems. As such, the ICS-specific guidance in Appendix I that is generally applicable to all information systems will be added to Appendix F during the next scheduled update to NIST Special Publication 800-53, Revision 3, projected for publication in December 2008.

AC-5 SEPARATION OF DUTIES

ICS Supplemental Guidance: In situations where the ICS cannot support the differentiation of roles or a single individual performs all roles within the ICS, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing measures) in accordance with the general tailoring guidance.

AC-6 LEAST PRIVILEGE

ICS Supplemental Guidance: In situations where the ICS cannot support differentiation of privileges or a single individual performs all roles within the ICS, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing measures) in accordance with the general tailoring guidance.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

ICS Supplemental Guidance: In situations where the ICS cannot support account/node locking or delayed login attempts, or the ICS cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., logging or recording all unsuccessful login attempts and alerting ICS security personnel though alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded) in accordance with the general tailoring guidance.

AC-8 SYSTEM USE NOTIFICATION

ICS Supplemental Guidance: In situations where the ICS cannot support system use notification, the organization employs appropriate compensating controls (e.g., posting physical notices in ICS facilities) in accordance with the general tailoring guidance.

AC-10 CONCURRENT SESSION CONTROL

ICS Supplemental Guidance: In situations where the ICS cannot support concurrent session control, the organization employs appropriate compensating controls (e.g., providing increased auditing measures) in accordance with the general tailoring guidance.

AC-11 SESSION LOCK

ICS Supplemental Guidance: The ICS employs session lock to prevent access to specified workstations/nodes. The ICS activates session lock mechanisms automatically after an organization-defined time period for designated workstations/nodes on the ICS. In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Session lock is not a substitute for logging out of the ICS. In situations where the ICS cannot support session lock, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance. NIST Special Publication 800-82 provides guidance on the use of session lock within an ICS environment.

AC-12 SESSION TERMINATION

ICS Supplemental Guidance: In situations where the ICS cannot support the automatic termination of remote sessions after a specified period of inactivity, or the ICS cannot automatically terminate remote sessions due to significant adverse impact on performance, safety, or reliability, the organization employs nonautomated mechanisms or procedures as compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms for reviewing user activities, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-15 AUTOMATED MARKING

ICS Supplemental Guidance: In situations where the ICS cannot support automated marking of output, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-16 AUTOMATED LABELING

ICS Supplemental Guidance: In situations where the ICS cannot support automated labeling of ICS information in process, in storage, or in transit, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-17 REMOTE ACCESS

ICS Supplemental Guidance: Remote access to ICS locations (e.g., control centers, field locations) is only enabled when necessary, approved, and authenticated. NIST Special Publication 800-82 defines and provides guidance on ICS remote access.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of remote access methods, the organization employs nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication [see IA-2 in this appendix], dial-in remote access may be enabled for a specified period of time or a call may be placed from the ICS site to the authenticated remote entity) in accordance with the general tailoring guidance.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing measures for remote sessions or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

AC-18 WIRELESS ACCESS RESTRICTIONS

ICS Supplemental Guidance: Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. In situations where the ICS cannot support the use of authentication or encryption to protect wireless access, or the components cannot use authentication or encryption due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing measures for wireless access or limiting wireless access) in accordance with the general tailoring guidance.

AWARENESS AND TRAINING

AT-2 SECURITY AWARENESS

ICS Supplemental Guidance: Security awareness training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

AT-3 SECURITY TRAINING

ICS Supplemental Guidance: Security training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security training program is consistent with the requirements of the security awareness and training policy established by the organization.

AUDITING AND ACCOUNTABILITY

AU-2 AUDITABLE EVENTS

ICS Supplemental Guidance: Most ICS auditing occurs at the application level. In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

ICS Supplemental Guidance: In general, audit record processing is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including response to audit failures, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

ICS Supplemental Guidance: In general, audit reduction and report generation is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including audit reduction and report generation, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENTS

CA-2 SECURITY ASSESSMENTS

ICS Supplemental Guidance: The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before an assessment can be conducted. If an ICS must be taken off-line to conduct an assessment, the assessment is scheduled to occur during planned ICS outages whenever possible. In situations where the organization cannot, for operational reasons, conduct a live assessment of a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct the assessment) in accordance with the general tailoring guidance.

CA-4 SECURITY CERTIFICATION

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (e.g., experienced in assessing ICS) authorized by the organization. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control.

CONFIGURATION MANAGEMENT

CM-3 CONFIGURATION CHANGE CONTROL

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on configuration change control for ICS.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to implement configuration change control, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-4 MONITORING CONFIGURATION CHANGES

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to enforce access restrictions and support auditing of enforcement actions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-6 CONFIGURATION SETTINGS

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-7 LEAST FUNCTIONALITY

ICS Supplemental Guidance: The organization considers disabling unused or unnecessary physical and logical ports and protocols (e.g., universal serial bus [USB], PS/2, FTP) on ICS components to prevent unauthorized connection of devices (e.g., thumb drives).

CONTINGENCY PLANNING

CP-2 CONTINGENCY PLAN

ICS Supplemental Guidance: The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the ICS executes predetermined procedures (e.g., alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, alert the operator and then maintain the last operational setting prior to failure). These examples are not exhaustive. NIST Special Publication 800-82 provides guidance on ICS failure modes.

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

ICS Supplemental Guidance: In situations where the organization cannot test or exercise the contingency plan on production ICS due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., using scheduled and unscheduled system maintenance activities including responding to ICS component and system failures, as an opportunity to test or exercise the contingency plan) in accordance with the general tailoring guidance.

CP-7 ALTERNATE PROCESSING SITE

ICS Supplemental Guidance: In situations where the organization cannot provide an alternate processing site, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

IDENTIFICATION AND AUTHENTICATION

IA-2 USER IDENTIFICATION AND AUTHENTICATION

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. In situations where the ICS cannot support user identification and authentication, or the organization determines it is not advisable to perform user identification and authentication due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance. For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access [see AC-17 in this appendix]. NIST Special Publication 800-82 provides guidance on ICS user identification and authentication.

Control Enhancements: (1) (2) (3)

ICS Enhancement Supplemental Guidance: Local and remote user access to ICS components is enabled only when necessary, approved, and authenticated. As defined in Appendix B, remote access refers to access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network. For ICS, the organization is the ICS owner/operator. Thus, remote access to the ICS is access from outside the system boundary defined by the ICS owner/operator. NIST Special Publication 800-82 defines and provides guidance on ICS remote access.

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

ICS Supplemental Guidance: In situations where the ICS cannot support device identification and authentication (e.g., serial devices), the organization employs compensating controls in accordance with the general tailoring guidance.

IA-4 IDENTIFIER MANAGEMENT

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based. NIST Special Publication 800-82 provides guidance on ICS identifier management.

IA-5 AUTHENTICATOR MANAGEMENT

ICS Supplemental Guidance: Many ICS devices and software are shipped with factory default authentication credentials to allow for initial installation and configuration. However, factory default authentication credentials are often well known, easily discoverable, present a great security risk, and therefore must be changed. Authentication may be role-based, group-based, or device-based. NIST Special Publication 800-82 provides guidance on ICS authenticator management.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

ICS Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

INCIDENT RESPONSE

IR-6 INCIDENT REPORTING

ICS Supplemental Guidance: Each organization establishes reporting criteria, to include sharing information through appropriate channels. The United States Computer Emergency Readiness Team (US-CERT) maintains the ICS Security Center at http://www.uscert.gov/control_systems. NIST Special Publication 800-82 provides guidance on ICS incident reporting.

MAINTENANCE

MA-3 MAINTENANCE TOOLS

Control Enhancement: (4)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot employ automated mechanisms to restrict the use of maintenance tools for the ICS, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

MA-4 REMOTE MAINTENANCE

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: In crisis or emergency situations, the organization may need immediate access to remote maintenance and diagnostic services in order to restore essential ICS operations or services. In situations where the organization may not have access to the required level of remote maintenance or diagnostic service provider security capability, the organization employs appropriate compensating controls (e.g., limiting the extent of the maintenance and diagnostic services to the minimum essential activities, and/or carefully monitoring and auditing the remote maintenance and diagnostic activities) in accordance with the general tailoring guidance.

PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-3 PHYSICAL ACCESS CONTROL

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to ICS facilities and assets to authorized individuals only. ICS are often constructed of devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan. NIST Special Publication 800-82 provides guidance on ICS physical access control.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

ICS Supplemental Guidance: This control applies to ICS communications infrastructure (e.g., satellite ground stations, microwave towers) within organizational facilities.

PE-6 MONITORING PHYSICAL ACCESS

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot employ automated mechanisms to recognize potential intrusions to the ICS and to initiate appropriate response actions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

PLANNING

PL-2 SYSTEM SECURITY PLAN

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on developing ICS security plans.

RISK ASSESSMENT

RA-2 SECURITY CATEGORIZATION

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on ICS security categorizations.

RA-3 RISK ASSESSMENT

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on ICS risk assessments.

RA-5 VULNERABILITY SCANNING

ICS Supplemental Guidance: Vulnerability scanning tools are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken off-line, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the organization cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct scanning) in accordance with the general tailoring guidance. NIST Special Publication 800-82 provides guidance on ICS vulnerability scanning.

SYSTEM AND SERVICES ACQUISITION

SA-4 ACQUISITIONS

ICS Supplemental Guidance: The SCADA and Control Systems Procurement Project provides example cyber security procurement language for ICS. See http://www.msisac.org/scada.

SA-8 SECURITY ENGINEERING PRINCIPLES

ICS Supplemental Guidance: NIST Special Publication 800-82 provides guidance on ICS defense-in-depth protection strategy.

SYSTEM AND COMMUNICATIONS PROTECTION

SC-3 SECURITY FUNCTION ISOLATION

ICS Supplemental Guidance: In situations where the ICS cannot support security function isolation, the organization employs compensating controls (e.g., providing increased auditing measures, limiting network connectivity) in accordance with the general tailoring guidance.

SC-7 BOUNDARY PROTECTION

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: Generally, public access to ICS information is not permitted.

SC-8 TRANSMISSION INTEGRITY

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-9 TRANSMISSION CONFIDENTIALITY

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-10 NETWORK DISCONNECT

ICS Supplemental Guidance: In situations where the ICS cannot terminate a network connection at the end of a session/specified time period of inactivity, or the ICS cannot terminate a network connection due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing measures) in accordance with the general tailoring guidance.

SC-13 USE OF CRYPTOGRAPHY

ICS Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-14 PUBLIC ACCESS PROTECTIONS

ICS Supplemental Guidance: Generally, public access to ICS is not permitted.

SC-15 COLLABORATIVE COMPUTING

ICS Supplemental Guidance: Generally, collaborative computing mechanisms are not permitted on ICS.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

ICS Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The use of Public Key Infrastructure technology in ICS is intended to support internal nonpublic use.

SC-19 VOICE OVER INTERNET PROTOCOL

ICS Supplemental Guidance: Generally, VoIP technologies are not permitted on ICS. The use of VoIP technologies is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SYSTEM AND INFORMATION INTEGRITY

SI-2 FLAW REMEDIATION

ICS Supplemental Guidance: NIST SP 800-82 provides guidance on flaw remediation in ICS.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage flaw remediation and automatic updates, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to conduct and report on the status of flaw remediation, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SI-3 MALICIOUS CODE PROTECTION

ICS Supplemental Guidance: The use of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS. NIST Special Publication 800-82 provides guidance on implementing ICS malicious code protection.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage malicious code protection mechanisms, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to update malicious code protection mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

ICS Supplemental Guidance: The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ICS.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

ICS Supplemental Guidance: Generally, it is not recommended to shut down and restart the ICS upon the identification of an anomaly.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms for the management of distributed security testing, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

ICS Supplemental Guidance: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ICS.

SI-8 SPAM PROTECTION

ICS Supplemental Guidance: The organization removes unused and unnecessary functions and services (e.g., electronic mail, Internet access). Due to differing operational characteristics between ICS and general purpose information systems, ICS do not generally employ spam protection mechanisms. Unusual traffic flow (e.g., during crisis situations), may be misinterpreted and detected as spam, which can cause issues with the ICS and possible system failure.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage spam protection mechanisms, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

Control Enhancements: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to update spam protection mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Proposed Information Collection; Comment Request; Cooperative Game Fish Tagging Report

AGENCY: National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

DATES: Written comments must be submitted on or before March 24, 2008.

ADDRESSES: Direct all written comments to Diana Hynek, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6625, 14th and Constitution Avenue, NW., Washington, DC 20230 (or via the Internet at *dHynek@doc.gov*).

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument and instructions should be directed to Eric Orbesen, (305) 361–4253 or *Eric.Orbesen@noaa.gov.*

SUPPLEMENTARY INFORMATION:

I. Abstract

The Cooperative Tagging Center, National Marine Fisheries Service (NMFS), NOAA attempts to determine the migration patterns and other biological information of billfish, tunas, and swordfish. Fishermen volunteer to tag and release their catch. The fish tagging report is provided to the angler with the tags, and he/she fills out the card with the information when a fish is tagged. Besides the tag number, the card request name, address, date, and club affiliation (if applicable). The card is then mailed back to NMFS where the data is stored.

II. Method of Collection

Information is submitted by mail.

III. Data

OMB Number: 0648–0247.
Form Number: NOAA form 88–162.
Type of Review: Regular submission.
Affected Public: Individuals or households.
Estimated Number of Respondents: 12,000.
Estimated Time per Response: 2 minutes.
Estimated Total Annual Burden Hours: 360.
Estimated Total Annual Cost to Public: $0.

IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: January 15, 2008.

Gwellnar Banks,

Management Analyst, Office of the Chief Information.

[FR Doc. E8–914 Filed 1–18–08; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Proposed Information Collection; Comment Request; Southeast Region Bycatch Reduction Device Certification Family of Forms

AGENCY: National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

DATES: Written comments must be submitted on or before March 24, 2008.

ADDRESSES: Direct all written comments to Diana Hynek, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6625, 14th and Constitution Avenue, NW., Washington, DC 20230 (or via the Internet at *dHynek@doc.gov*).

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument and instructions should be directed to Jason Rueter, (727) 824–5350 or *jason.rueter@noaa.gov.*

SUPPLEMENTARY INFORMATION:

I. Abstract

Any person seeking to obtain certification for bycatch reduction devices (BRD) to be used on shrimp vessels in the Gulf of Mexico or South Atlantic must apply for authorization to conduct tests and submit the test results. Persons seeking certification to be observers for such tests in the Gulf of Mexico must file an application and provide three references. The information is needed for NOAA to determine if the equipment meets the standards that would allow its use in commercial fisheries.

II. Method of Collection

Paper applications and telephone calls are required from participants, and methods of submittal include mailing and facsimile transmission of paper forms.

III. Data

OMB Number: 0648–0345.
Form Number: None.
Type of Review: Regular submission.
Affected Public: Individuals or households; business or other for-profit organizations.
Estimated Number of Respondents: 32.
Estimated Time per Response: Pre-certification and certification applications, 2 hours and 20 minutes; pre-certification data collection, 3 hours; vessel information form, trip report/cover sheet and duplication/mailing of independent BRD tests, 30 minutes; gear specification form, station sheet and station sheet tuning forms, Turtle Excluder Device/BRD specification form, length frequency form, condition and fate form, 20 minutes; species characterization form and program receipt form, 5 hours; sea turtle form, 15 minutes; final reports, 4 hours; testing, 4 hours; observer certifications and observer references, 1 hour.
Estimated Total Annual Burden Hours: 6,899.
Estimated Total Annual Cost to Public: $306,495 in capital and recordkeeping/reporting costs.

IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information

is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: January 15, 2008.

Gwellnar Banks,

Management Analyst, Office of the Chief Information Officer.

[FR Doc. E8–915 Filed 1–18–08; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Proposed Information Collection; Comment Request; Southeast Region Gear Identification Requirements

AGENCY: National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

DATES: Written comments must be submitted on or before March 24, 2008.

ADDRESSES: Direct all written comments to Diana Hynek, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6625, 14th and Constitution Avenue, NW., Washington, DC 20230 (or via the Internet at *dHynek@doc.gov*).

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument and instructions should be directed to Jason Rueter, (727) 824–5350 or *jason.rueter@noaa.gov*.

SUPPLEMENTARY INFORMATION:

I. Abstract

The participants in Federally-regulated fisheries in the Southeast Region of the U.S. must mark their fishing gear with the official identification number or some other form of identification and color code. Harvesters of aquaculture live rock must mark or tag the material deposited. This identification is necessary to aid fishery enforcement activities and for purposes of gear identification concerning damage, loss, and civil proceedings.

II. Method of Collection

No information is collected.

III. Data

OMB Number: 0648–0359.

Form Number: None.

Type of Review: Regular submission.

Affected Public: Individuals or households; and business or other for-profits organizations.

Estimated Number of Respondents: 1,000.

Estimated Time per Response: 7 minutes for traps; 10 seconds for live rock; and 20 minutes for mackerel gillnets.

Estimated Total Annual Burden Hours: 2,192.

Estimated Total Annual Cost to Public: $17,000 in capital and recordkeeping/reporting costs.

IV. Request for Comments

Comments are invited on: (a) Whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and cost) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: January 15, 2008.

Gwellnar Banks,

Management Analyst, Office of the Chief Information Officer.

[FR Doc. E8–916 Filed 1–18–08; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Proposed Information Collection; Comment Request; Southeast Region Vessel Identification Requirements

AGENCY: National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burden, invites the general public and other Federal agencies to take this opportunity to comment on proposed and/or continuing information collections, as required by the Paperwork Reduction Act of 1995.

DATES: Written comments must be submitted on or before March 24, 2008.

ADDRESSES: Direct all written comments to Diana Hynek, Departmental Paperwork Clearance Officer, Department of Commerce, Room 6625, 14th and Constitution Avenue, NW., Washington, DC 20230 (or via the Internet at *dHynek@doc.gov*).

FOR FURTHER INFORMATION CONTACT: Requests for additional information or copies of the information collection instrument and instructions should be directed to Jason Rueter, (727) 824–5350 or *jason.rueter@noaa.gov.*

SUPPLEMENTARY INFORMATION:

I. Abstract

The participants in federally-regulated fisheries in the Southeast Region of the U.S. must mark their fishing vessels with the official identification number or some other form of identification. The vessel's identification number is displayed on its deckhouse or hull, and its weatherdeck. This identification is necessary to aid fishery enforcement activities and for purposes of gear identification concerning damage, loss, and civil proceedings.

II. Method of Collection

No information is collected.

III. Data

OMB Number: 0648–0358.

Form Number: None.

Type of Review: Regular submission.

Affected Public: Individuals or households; business or other for-profits organizations.

Estimated Number of Respondents: 9,774.

Estimated Time per Response: 45 minutes.