FY 2005 Instructions for Preparing the Federal Information Security Management Act Report and Privacy Management Report

Table of Contents

Section A - Instructions for Completing the Annual Federal Information Security Management Act (FISMA) Report and Privacy Management Report

This section contains instructions for FY 05 FISMA and privacy reporting. The reporting templates are contained in Sections B, C, and D. Each of the templates are to be completed by the appropriate agency officials, as part of one combined report signed by the agency head and transmitted to the Director, Office of Management and Budget (OMB) by October 7, 2005. In addition to formal transmission, an electronic copy of the report should be sent to fisma@omb.eop.gov .

Each agency head's annual report to OMB shall comprise:

1. Transmittal letter from the agency head, including a discussion of any differences between the findings of the agency CIO and IG.

2. Section B Template completed by the CIO - Results of annual IT security reviews of systems and programs.

3. Section C Template completed by the IG - Results of the IG independent evaluation.

4. Section D Template completed by the Senior Agency Official for Privacy - Status of agency compliance with OMB privacy policies.

When to send reports to Congress and the Government Accountability Office (GAO):

> After review by and notification from OMB, agencies shall forward their transmittal letter with report sections B and C to the appropriate Congressional Committees and GAO. Transmittal of agency reports to Congress shall be made by, or be consistent with guidance from, the agency's Congressional or Legislative Affairs office to the following: Committees on Government Reform and Science of the House, the Committees on Government Affairs and Commerce, Science, and Transportation of the Senate, and the Congressional authorization and appropriations committees for each individual agency. In prior years, the Committees have provided to OMB specific points of contact for receiving the reports. As in the past, if such are provided to OMB, we will notify the agencies.

Agency responses shall be based on the results of the annual system and program reviews, the agency's work in correcting weaknesses identified in their POA&Ms, and any other work performed throughout the reporting period. Extensive narrative responses are strongly discouraged, but agencies may provide brief comments in the space provided. IGs are however encouraged to provide any additional narrative in an appendix to the report to the extent they provide meaningful insight into the status of the agency's security or privacy program.

If an agency has developed additional performance measures beyond those provided by OMB, they may report them as well. However, incomplete reporting on OMB's performance measures will be noted in OMB's public report to Congress and will be a consideration in OMB's annual approval or disapproval of the agency's security program. When completing the reporting template, agencies may find it useful to refer to the definitions contained in Section C of the FY 04 FISMA reporting guidance.

When agency CIO and IG findings do not agree, the agency head's transmittal letter to the OMB Director shall identify and summarize the disagreements and explain why they cannot be reconciled.

The table below outlines the FY 05 FISMA questions that represent a significant change from the FY 04 FISMA Reporting Instructions (OMB M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, August 2004). All questions for the Senior Agency Official for Privacy (Section D) are new in the FY 05 guidance. The privacy program questions in this document will replace questions that were formerly part of your agency's annual E-Government Act report.

	New Questions	**Significantly Changed Questions**	**No Significant Changes**
CIO, Section B	3. – Use of NIST 800-53. 10. – Emerging Technologies.	1. and 2. – Reporting by FIPS category. 4. – Incident detection capabilities now focuses on use of tools. 5. – Changed incident categories to mirror NIST guidance.	6. and 7. – Training. 8. – Configuration Management. 9. – Incident Response.
IG, Section C		1. and 2. – Reporting by FIPS category. 3. – Question asks whether E-authentication risk assessments are completed. 4. - POA&M evaluation. Some elements of the question were deleted from last year's instructions (see below).	3. – Contractor Oversight, system inventory. 5. – C&A evaluation. 6. – Configuration Management. 7. – Incident Response. 8. and 9. - Training.

Questions deleted from the FY 04 FISMA Reporting Instructions:

A.1.a. – Number of programs.

A.2.b. – Number of systems with security control costs integrated into the life cycle of the system.

A.2.d. - Number of systems with a contingency plan.

A.3.b. – Reviews of programs, systems, and contractor operations or facilities were conducted using the NIST self-assessment guide, 800-26.

A.3.c. – In instances where the NIST self assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.

A.3.e. – The OIG was included in the development and verification of the agency's IT system inventory.

A.3.g. – The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.

A.3.i. – The agency has appointed a senior agency information security officer that reports directly to the CIO.

B.1. – By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY 03. In addition, for each significant deficiency, indicate whether a POA&M has been developed.

C.1.d. – CIO develops, implements, and manages POA&M's for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.

C.1.f. – The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.

C.1.g. – System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).

C.1.h. – OIG has access to POA&Ms as requested.

D.2. – Evaluate the degree to which configuration requirements address the patching of security vulnerabilities.

E.2.a. – How many systems underwent vulnerability scans and penetration tests in FY 04?

F.2.a., F.2.b – Number of systems affected, by category, on: systems with a complete and up-to-date C&A, and systems without complete and up-to-date C&A.

F.2.c. – How many successful incidents occurred for known vulnerabilities for which a patch was available?

Frequently Asked Questions

Security Reporting – Questions 1 through 21; pp. 4-10.
Privacy Reporting– Questions 22 through 25; pp. 10-11.

Security Reporting

1. *What systems should be reported under FISMA?*
   FISMA applies to information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. All systems meeting this definition shall be included in the report.

2. *There are no instructions for quarterly performance metric updates. Are agencies still required to submit a quarterly update to OMB?*
   Yes. Quarterly updates are still required, and will be due on September 15, 2005; December 15, 2005; March 15, 2006; and June 15, 2006. Instructions and reporting format will be sent to agency CIOs at a later date, and will be posted on the OMB website.

3. *Is use of National Institute of Science and Technology (NIST) publications required?*
   Yes. For non-national security programs and systems, agencies must follow NIST standards and guidance.

4. *Must agencies report at both an agency wide level and by individual component?*
   Yes. Agencies must provide an overall agency view of their security program, but most of the topic areas also require specific responses for each of the major components (e.g., bureaus or operating divisions). Thus, the agencies' and OMB's report can distinguish good performing components from poor performers and more accurately reflect the overall agency performance. For agencies with extensive field and regional offices, it is not necessary to report to OMB on the performance of each of the field offices. Rather, agencies shall confirm the security program of the major component which operates the field offices: 1) is effectively overseeing and measuring field performance; 2) is including any weaknesses in the agency wide POA&M, and; 3) is developing, implementing, and maintaining system POA&Ms.

5. *When should program officials and CIOs provide the results of their reviews to the IG?*
   Program officials and CIOs should share the findings from program and system security reviews with their IG as they become available throughout the year.

6. *Do all agency systems have to be reviewed annually?*
   Yes. Senior agency program officials and CIOs must review all systems at least annually. Only the depth and breadth of such system reviews are flexible.

7. *What level of review is required for an individual system?*
Program officials and CIOs are responsible for reviewing the security of all systems under their respective control. Clearly, the necessary depth and breadth of an annual system review depends on several factors such as: 1) the potential risk and magnitude of harm to the system or data; 2) the relative comprehensiveness of last year's review; and 3) the adequacy and successful implementation of the POA&M for weaknesses in the system. For example, if last year a system underwent a complete certification and accreditation (consistent with NIST or national security guidance), this year a relatively simple update or maintenance review may be sufficient, provided it has been adequately documented within the agency. An effective security program demands comprehensive and continuous understanding of program and system weaknesses. At a minimum, agency program officials and CIOs must take into account the three criteria listed above in determining the appropriate level of annual review. IGs may report on the adequacy of such reviews.

8. *What methodology must agencies use to review systems?*
This year, agencies can:

   1) Continue to use NIST Special Publication 800-26, "Security Self- Assessment Guide for Information Technology Systems" (November 2001), or,

   2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" (February, 2005).

9. *What reporting is required for national security systems?*
FISMA requires annual reviews and reporting of all systems, including national security systems. Agencies can choose to provide responses to the questions in the template either in aggregate with or separate from their non-national security systems.

   Agencies shall describe how they are implementing the requirements of FISMA for national security systems in their report. The description shall include the extent to which the management and internal oversight of an agency's national security programs and systems are being handled differently than the program for non-national security programs and systems and why. DoD and the Director of National Intelligence shall report on compliance with their policies and guidance.

   The intelligence community CIO reports on systems processing or storing sensitive compartmentalized information (SCI) across the intelligence community and those other systems for which the Director of National Intelligence is the principal accrediting authority. Agencies shall follow the intelligence community reporting guidance for these systems. SCI systems shall only be reported via the intelligence community report. However, this separate reporting does not alter an agency head's responsibility for overseeing the security of all operations and assets of the agency or component. Therefore, copies of separate reporting must also be provided to the agency head for their use.

To assist oversight by appropriate national security authorities, it is important to specify where practicable which portion of the agency report pertains to national security systems.

10. *What are minimally acceptable system configuration requirements?*
FISMA (section 3544(b)(2)(D)(iii)) requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Systems with secure configurations have fewer vulnerabilities and are better able to thwart network attacks.

    A number of commercial and government-owned products are available for configuring and testing software for adherence to security configuration requirements. Agencies are to cite in their report the frequency by which they implement system configuration requirements.

11. *Why must agencies explain their performance metrics in terms of FIPS 199 categories?*
FISMA tasked NIST to develop a standard to categorize all information and information systems based upon the need to provide appropriate levels of information security according to a range of risk levels. FIPS Publication 199, "Federal Information Processing Standard 199: Standards for Security Categorization of Federal Information and Information Systems" (February 2004) defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). These impact levels are: low, moderate and high. All agencies must categorize their information and information systems using one of these three categories in order to determine which security controls in NIST Special Publication 800-53 should be implemented.

12. *How often do I need to test and evaluate my security controls?*
At least annually. FISMA (section 3544(b)(5)) requires each agency to perform for all systems "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually." This evaluation shall include the testing of management, operational, and technical controls.

13. *You are no longer asking agencies to report significant deficiencies in the annual FISMA report. Don't we have to report them?*
Yes, but not in the annual FISMA report to OMB. FISMA requires agencies to report a significant deficiency: 1) as a material weakness under FMFIA, or 2) as an instance of a lack of substantial compliance under FFMIA, if related to financial management systems. See OMB Circular A-123 for further information on reporting significant deficiencies. As you know, all security weaknesses (including those identified as a significant deficiency or material weakness) must be included in and tracked on your plan of actions and milestones.

A significant deficiency is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

14. *Must government contractors abide by FISMA requirements?*
Yes. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires each agency 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."

Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency IT security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local governments, industry partners, etc. FISMA, therefore, underscores longstanding OMB policy concerning sharing government information and interconnecting systems. Therefore, Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III). Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data.
Agencies must also review the security of other users with privileged access to Federal data and systems.

Finally, because FISMA applies to Federal information (in addition to information systems), in certain limited circumstances its requirements also apply to a specific class of information technology to which Clinger-Cohen did not, i.e., "equipment that is acquired by a Federal contractor incidental to a Federal contract." Therefore, when Federal information is used within incidentally acquired equipment, the agency is responsible for ensuring FISMA requirements are met.

15. *Could you provide examples of IT acquired "incidental" to a contract and thus not subject to FISMA?*
Again, in considering the answer to this question, it is essential to remember FISMA requires agencies to provide security protections "...commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or other organization on behalf of an agency."

A corporate human resource or financial management system acquired solely to assist managing corporate resources assigned to a government contract could be incidental, provided the system does not use agency information or interconnect with an agency system.

16. *Could you provide examples of agency security responsibilities concerning contractors and other sources?*
In considering the answer to this question, it is essential to remember FISMA requires agencies to provide security protections "...commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or other organization on behalf of an agency."

While we cannot anticipate all possible combinations and permutations, there are three primary categories of contractors as they relate to securing systems and information: 1) service providers, 2) contractor support, and 3) Government Owned, Contractor Operated facilities (GOCO).

1) Service providers -- this encompasses typical outsourcing of system or network operations, telecommunications services, or other managed services.

   Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. For example, annual reviews, risk assessments, security plans, control testing, contingency planning, and certification and accreditation must, at a minimum, explicitly meet guidance from NIST. Additionally, IGs shall include some contractor systems in their "representative subset of agency systems," and not doing so presents an incomplete independent evaluation.

2) Contractor support -- this encompasses on or offsite contractor technical or other support staff.

   Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. Specifically, the agency is responsible for ensuring the contractor personnel receive appropriate training (i.e., general and specific).

3) Government Owned, Contractor Operated (GOCO) -- For the purposes of FISMA, GOCO facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in the terms of the contract.

17. *How do agencies ensure FISMA compliance for connections to non-agency systems?*

    NIST SP 800-47 "Security Guide for Interconnecting Information Technology Systems" (August, 2002) provides a management approach for interconnecting IT systems, with an emphasis on security. The document recommends development of an Interconnection Security Agreement (ISA) and a Memorandum of Understanding (MOU). The ISA specifies the technical and security requirements of the interconnection, and the MOU defines the responsibilities of the participating organizations. The security guide recommends regular communications between the organizations throughout the life cycle of the interconnection. One or both organizations shall review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure the controls are operating properly and are providing appropriate levels of protection.

    Security reviews may be conducted by designated audit authorities of one or both organizations, or by an independent third party. Both organizations shall agree on the rigor and frequency of reviews as well as a reporting process.

18. *OMB asks agencies whether they have provided IT security training and awareness to all employees, including contractors. Is it the agency's responsibility to ensure contractors have security training if they are hired to perform IT security functions? Wouldn't they already be trained by their companies to perform this work?*

    The agency should include in its contract the requirements for level of skill and experience. However, contractors must be briefed on agency security policies and procedures, including rules of behavior. Agencies may explain the type of awareness training they provide to contractors as part of the response to section e. of Question 6.

19. *Why did you change the incident categories?*

    They were changed to reflect the incident categories described in NIST Special Publication 800-61, “Computer Security Incident Handling Guide” (January, 2004).

20. *What is the link between the E-Authentication Risk Assessment and the FISMA Risk Assessment and Certification and Accreditation Security Requirements?*

    The E-Authentication Guidance for Federal Agencies established the requirement for agencies to conduct an e-authentication risk assessment on systems remotely authenticating users over a network for purposes of e-government and commerce.

    On December 16, 2003 OMB issued M-04-04, “E-Authentication Guidance for Federal Agencies.” As stated in M-04-04, agencies must categorize all existing transactions/systems requiring user authentication into one of the described assurance levels by September 15, 2005.

    E-authentication risk assessment should be conducted in parallel with the overall system risk assessment and in the context of greater policy issues, and should be conducted with the advice of agency legal, policy, privacy, and agency business

process owners. Additionally, agencies shall address the requirements of M-04-04 in their System Security Plans and certify the requirements prior to authorization to process.

21. *Why is OMB asking about Peer to Peer file sharing in IT security training?*
IT security awareness training should evolve as emerging technologies enter into the workplace. A type of file sharing (known as Peer to Peer or P2P) generally refers to any software or system allowing individual users of the Internet to connect to each other and trade computer files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. While there are many appropriate uses of this technology, a number of studies show the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for the spread of computer viruses within IT systems.

Federal computer systems, as well as those operated by contractors on the government's behalf, must not be used for the downloading of illegal and/or unauthorized copyrighted content, including illegal downloads using file sharing programs. Further information is detailed in the Chief Information Officers Council's recommended guidance on "Limited Personal Use of Government Office Equipment Including Information Technology[1]". Agency policies and training programs shall be consistent with the CIO Council guidance.

Privacy Reporting

22. *Which agency official should complete the privacy questions in this FISMA report?*
These questions shall be completed by the Senior Agency Official for Privacy. Since privacy management may fall into areas of responsibility likely held by several program officials, *e.g.*, the CIO, the Privacy Act Officer, etc., the Senior Agency Official for Privacy shall consult with these officials when responding to these questions, and note (Section IV) those who contributed and/or reviewed the responses to the questions.

23. *Why is OMB asking some of the same privacy questions posed by the annual E-Government Act Report?*
OMB is using the FISMA reporting vehicle to aggregate privacy reporting requirements and reduce burden on the agencies. Privacy reporting in Section D will satisfy agencies' privacy reporting obligations under the E-Government Act. OMB will not include privacy reporting in the E-Government Act reporting template.

24. *Should the IGs answer the privacy questions?*
OMB encourages IGs to provide any meaningful data they have regarding the agency's privacy program and related activities. IGs may submit this information to OMB along with the agency's response to Section D, or they may separately submit

[1] http://www.cio.gov/documents/peruse_model_may_1999.pdf (May 19, 1999)

additional comments as an appendix to the report. However, this information shall not be included in the IG's report to Congress or GAO.

25. *Will OMB send agencies' privacy reporting (Section D) to Congress as part of the FISMA report?*
No. OMB's FISMA report to Congress will address only agencies' FISMA reporting (templates B & C). When agencies and IGs send reports to Congress and GAO, they should not include the privacy section.

Section B - Reporting Template for Agency CIOs

A reporting template tool will be sent at a later date, and will be posted at http://www.omb.gov . Below are the questions to be included in the template, in a narrative format.

Questions in the excel template require mostly numerical responses, and must follow the prescribed format provided. Please do not alter the questions or the reporting template. Comments and narrative to accompany quantitative answers should be provided in the comment area following each question, but, only if appropriate or necessary.

1. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of information systems used or operated by your agency, and the number of information systems used or operated by a contractor of your agency or other organization on behalf of your agency.

   Note: Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

   To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:

   1) Continue to use NIST Special Publication 800-26, or,
   2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

   Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

   FIPS 199, a Federal information processing standard, was published in February 2004. **If there are systems which have not yet been categorized, or, if a risk impact level was determined through another method, please explain below in item (d.).**

   a. FY 05 Agency Systems
   - By bureau: total number, number evaluated
   - By FIPS 199 impact level (high, moderate, low, not categorized): total number, number evaluated

   b. FY 05 Contractor Systems
   - By bureau: total number, number evaluated

- By FIPS 199 impact level (high, moderate, low, not categorized): total number, number evaluated

c. FY 05 Total Number of Systems
- By bureau: total number of agency systems and contractor systems, number evaluated
- By FIPS 199 impact level (high, moderate, low, not categorized): total number, number evaluated

d. If there are systems which have not yet been categorized, or, if a risk impact level was determined through another method, please explain.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the Total Number of Systems, identify the number of systems which have: a current certification and accreditation[2], a contingency plan tested within the past year, and security controls tested within the past year.

Contingency planning is a requirement for certification and accreditation, with annual contingency plan testing required thereafter. If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain.

a. Number of systems certified and accredited
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

b. Number of systems for which security controls have been tested and evaluated in the last year
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

c. Number of systems for which contingency plans have been tested in accordance with policy and guidance
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

d. If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain.

[2] Certification and accreditation requires documentation of security planning, including: risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements.

3. Agencies must implement the recommended security controls in NIST Special Publication 800-53.

a. Do you have a plan in place to fully implement the security controls recommended in NIST Special Publication 800-53? Yes or No.
b. Have you begun to implement the security controls recommended in NIST Special Publication 800-53? Yes or No.

4. Incident Detection Capabilities.

a. What tools, techniques, technologies, etc., does the agency use for incident detection?
b. How many systems (or networks of systems) are protected using the tools, techniques and technologies described above?

5. Information gathered in this question will be forwarded to the Department of Homeland Security for validation.

For each category of incident listed: identify the total number of successful incidents in FY 05, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category e., "Other". If appropriate or necessary, include comments in the area provided below.

a. Unauthorized Access
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

b. Denial of Service (DoS)
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

c. Malicious Code
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

d. Improper Usage
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

e. Other
- Number reported internally
- Number reported to US-CERT

- Number reported to law enforcement

Comments: Space provided for narrative comments.

6. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Yes or No.

a. Total number of employees in FY 05

b. Number of employees that received IT security awareness training in FY 05, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003)

c. Total number of employees with significant IT security responsibilities

d. Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998).

e. Briefly describe the training provided in b. and d.

Comments: Space provided for narrative comments.

7. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.

8. Configuration Management.

a. Is there an agency wide security configuration policy? Yes or No.
Comments: Space for narrative comments.

b. Configuration guides are available for the products listed below. With a checkmark, identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

□ Windows XP Professional

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Windows NT

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Windows 2000 Professional

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Windows 2000 Server

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Windows 2003 Server

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Solaris

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ HP-UX

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Linux

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Cisco Router IOS

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Oracle

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software

- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□Other. Specify:

9. Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

a. The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.

Comments: Space provided for narrative comments.

10. New Technologies and Emerging Threats

a. Has the agency documented in its security policies special procedures for using emerging technologies (including but not limited to wireless and IPv6) and countering emerging threats (including but not limited to spyware, malware, etc.)?
Yes or No.

b. If the answer to 10 a. is "Yes," briefly describe the documented procedures. These special procedures could include more frequent control tests & evaluations, specific configuration requirements, additional monitoring, or specialized training.

Section C – Reporting Template for Agency IGs

A reporting template tool will be sent at a later date, and will be posted at http://www.omb.gov . Below are the questions to be included in the template, in a narrative format.

Questions in the excel template require mostly numerical responses, and must follow the prescribed format provided. Please do not alter the questions or the reporting template. Comments and narrative to accompany quantitative answers should be provided in the comment area following each question, but, only if appropriate or necessary. IGs may also submit additional narrative in an appendix to the report.

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

   To meet the annual requirement for conducting a NIST Special Publication 800-26 review, agencies can:

   1) Continue to use NIST Special Publication 800-26, or,
   2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53 "Recommended Security Controls for Federal Information Systems"

   Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

   a. FY 05 Agency Systems
   - By bureau
   - By FIPS 199 impact level (high, moderate, low, not categorized).

   b. FY 05 Contractor Systems
   - By bureau
   - By FIPS 199 impact level (high, moderate, low, not categorized).

   c. FY 05 Total Number of Systems
   - By bureau
   - By FIPS 199 impact level (high, moderate, low, not categorized).

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the

following: have a current certification and accreditation[3], a contingency plan tested within the past year, and security controls tested within the past year.

a. Number of systems certified and accredited
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

b. Number of systems for which security controls have been tested and evaluated in the last year
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

c. Number of systems for which contingency plans have been tested in accordance with policy and guidance
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

3. In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

a. The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.

Response Categories:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

b. The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

Response Categories:
- Approximately 0-50% complete
- Approximately 51-70% complete

[3] Certification and accreditation requires documentation of security planning, including: risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements.

- Approximately 71-80% complete
- Approximately 81-95% complete
- Approximately 96-100% complete

c. The OIG **generally** agrees with the CIO on the number of agency owned systems. Yes or No.
d. The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.
e. The agency inventory is maintained and updated at least annually. Yes or No.
f. The agency has completed system e-authentication risk assessments. Yes or No.

4. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

a. The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.

Response Categories:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

b. When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).

Response Categories:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

c. Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.

Response Categories:
- Rarely, for example, approximately 0-50% of the time

- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

d. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.

Response Categories:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

e. OIG findings are incorporated into the POA&M process.

Response Categories:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

f. POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.

Response Categories:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

Comments: Space provided for narrative comments.

5. OIG Assessment of the Certification and Accreditation Process

OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as

associated NIST documents used as guidance for completing risk assessments and security plans[4].

Assess the overall quality of the Department's certification and accreditation process.

Response Categories:
- Excellent
- Good
- Satisfactory
- Poor
- Failing

Comments: Space for narrative comments.

6. Configuration Management.

a. Is there an agency wide security configuration policy? Yes or No.
Comments: Space for narrative comments.

b. Configuration guides are available for the products listed below. With a checkmark, identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

□ Windows XP Professional

Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Windows NT

Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software

[4] Certification and accreditation requires documentation of security planning, including: risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements.

- Almost Always, or on approximately 96-100% of the systems running this software

□ Windows 2000 Professional
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Windows 2000 Server
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Windows 2003 Server
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Solaris
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ HP-UX

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Linux

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Cisco Router IOS

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Oracle

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Other. Specify:

7. Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

   a. The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.
   b. The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.
   c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.

   Comments: Space provided for narrative comments.

8. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?
   - Rarely, or, approximately 0-50% of employees have sufficient training
   - Sometimes, or approximately 51-70% of employees have sufficient training
   - Frequently, or approximately 71-80% of employees have sufficient training
   - Mostly, or approximately 81-95% of employees have sufficient training
   - Almost Always, or approximately 96-100% of employees have sufficient training

9. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.

Section D - Reporting Template for Senior Agency Officials for Privacy

A reporting template tool will be sent at a later date. Below are the questions to be included in the template, in a narrative format. This shall be completed by all agencies.

I. Senior Agency Official for Privacy Responsibilities

1. Can your agency demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)?
Yes or No.

2. Can your agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19?
Yes or No.

3. Can your agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information?
Yes or No.

II. Procedures and Practices

1. Does your agency have a training program to ensure that all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure?
Yes or No.

2. Does your agency have a program for job-specific information privacy training (i.e., detailed training for individuals (including contractor employees) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities)?
Yes or No.

3. Section 3, Appendix 1 of OMB Circular A-130 requires agencies conduct -- and be prepared to report to the Director, OMB on the results of -- reviews of activities mandated by the Privacy Act.
Please indicate by component (e.g., bureau, agency) which of the following reviews were conducted in the last fiscal year.
[make chart with the following headings]

Section M Contracts	Records Practices	Routine Uses	Exemptions	Matching Programs	Training	Violations	Systems of Records

4. Section 208 of the E-Government Act requires that agencies (a.) conduct Privacy Impact Assessments under appropriate circumstances, (b.) post web privacy policies on their websites, and (c.) ensure machine-readability of web privacy policies.

a. Does you agency have a written process or policy for:

(i) determining whether a PIA is needed?	Yes/No
(ii) conducting a PIA?	Yes/No
(iii.) evaluating changes in business process or technology that the PIA indicates may be required?	Yes/No
(iv.) ensuring that systems owners and privacy and IT experts participate in conducting the PIA?	Yes/No
(v.) making PIAs available to the public in the required circumstances?	Yes/No
(vi.) making PIAs available in other than required circumstances?	Yes/No

b. Does your agency have a written process for determining continued compliance with stated web privacy policies?
Yes or No.

c. Do your public-facing agency web sites have machine-readable privacy policies (i.e., are your web privacy policies P3P-enabled or automatically readable using some other tool)?
Yes or No.

(i.) if not, provide date for compliance:

5. By bureau, identify the number of information systems containing Federally-owned information in an identifiable form. For the applicable systems, on how many have you conducted a Privacy Impact Assessment and published a Systems of Records Notice?

a. FY 05 Systems that contain Federally-owned information in an identifiable form

- By bureau: number that contain information in an identifiable form
  - Agency Systems
  - Contractor Systems
  - Total number of systems

b. FY 05 Privacy Impact Assessments

- By bureau: total number requiring a Privacy Impact Assessment in FY 05 (systems that are new or have been substantially altered)
  - Agency Systems
  - Contractor Systems
  - Total number of systems

- By bureau: number that have a completed Privacy Impact Assessment within FY 05
  - Agency Systems
  - Contractor Systems
  - Total number of systems

c. FY 05 Systems of Records Notices
- By bureau: number of systems from which Federally-owned information is retrieved by name or unique identifier
  - Agency Systems
  - Contractor Systems
  - Total number of systems

- By bureau: number of systems for which one or more Systems of Records Notice/s have been published in the Federal register
  - Agency Systems
  - Contractor Systems
  - Total number of systems

d. Contact Information for preparer of question 5.

6. OMB policy (Memorandum 03-22) prohibits agencies from using persistent tracking technology on web sites except in compelling circumstances as determined by the head of the agency (or designee reporting directly to the agency head).

a. Does your agency use persistent tracking technology on any web site?
Yes/No
b. Does your agency annually review the use of persistent tracking?
Yes/No
c. Can your agency demonstrate through documentation the continued justification for and approval to use the persistent technology?
Yes/No
d. Can your agency provide the notice language used or cite to the web privacy policy informing visitors about the tracking?
Yes or No.

III. Internal Oversight

1. Does your agency have current documentation demonstrating review of compliance with information privacy laws, regulations and policies?
Yes or No.
(i.) If so, provide the date the documentation was created.

2. Can your agency provide documentation demonstrating corrective action planned, in progress or completed to remedy identified compliance deficiencies?
Yes or No.
(i.) If so, provide the date the documentation was created.

3. Does your agency use technologies that allow for continuous auditing of compliance with stated privacy policies and practices?
Yes or No.

4. Does your agency coordinate with the agency Office of Inspector General on privacy program oversight by providing to OIG the following materials:

a. compilation of the agency's privacy and data protection policies and procedures? Yes/No
b. summary of the agency's use of information in identifiable form? Yes/No
c. verification of intent to comply with agency policies and procedures? Yes/No

5. Does your agency submit an annual report to Congress (OMB) detailing your privacy activities, including activities under the Privacy Act and any violations that have occurred?
Yes or No.
(i.)If so, when was this report submitted to OMB for clearance?

IV. Contact Information

Please provide the names, phone numbers, and e-mail addresses of the following officials:

Agency head:

Chief Information Officer:

Agency Inspector General:

Chief Information Security Officer:

Senior Agency Official for Privacy:

Chief Privacy Officer:

Privacy Advocate:

Privacy Act Officer:

Reviewing Official for PIAs: