# 5 FAM 1060 INFORMATION ASSURANCE MANAGEMENT

*(CT:IM-103;   01-23-2009)*
*(Office of Origin:  IRM/IA)*

## 5 FAM 1061  GENERAL

*(CT:IM-82;   02-22-2007)*

a. The Chief Information Security Officer (CISO) operates under the direction and supervision of the Chief Information Officer (CIO).  The CISO is responsible for defining and evaluating the information security posture of the Department's information and information systems (see 1 FAM 272).

b. Acting for the CIO, the CISO oversees all Department information security elements.  As part of this oversight, the CISO will determine the level of information security necessary to protect the Department's information as directed by 44 U.S.C. 3544 (see 5 FAM 110).

c. Within the context of this policy, the use of the term "information security" applies to the security of all Department information processed or stored in electronic form on behalf of the Department or processed or stored on a Department information system.

d. See 5 FAH-11 H-014 for terms and definitions related to information assurance functions specified in this subchapter.

## 5 FAM 1062  AUTHORITIES

*(CT:IM-82;   02-22-2007)*

This section contains the authorities and references for this chapter.

### 5 FAM 1062.1  Legislation and Regulations

*(CT:IM-103;   01-23-2009)*

*a.* Public Law 107-305, Cyber Security Research and Development Act of 2002

*b.* Public Law 107-296, The Homeland Security Act of 2002 (November 25, 2002) *c.* Public Law 103-62, Government Performance Act of 1993

*d.* Public Law 104-231, Information Technology Management Reform Act of 1996, October 2, 1996

*e.* Public Law 105-220, Section 508 Accessibility, August 1998

*f.* Clinger-Cohen Act, February 10, 1996 (Divisions D & E of Public Law 104-106)

*g.* Paperwork Reduction Act 1995

*h.* Government Paperwork Elimination Act – Public Law 105-277, Title XVII

*i.* Federal Acquisition Reform Act of 1995

*j.* Federal Acquisition Streamlining Act of 1994 and Simplified Acquisition Threshold Acquisitions

*k.* Federal Information Security Management Act of 2002 (Title III of Public Law 107-347)

*l.* E-Government Act of 2002 (Public Law 107-347)

*m.* The Freedom of Information Act, 5 U.S.C. 552, As Amended By Public Law 104-231, 110 Stat. 3048

*n.* Privacy Act of 1974, 5 U.S.C. 522A

*o.* Inspector General Act of 1978, 5 U.S.C., App.3, as amended

*p.* Foreign Service Act of 1980, Section 209, 22 U.S.C. 3929, as amended

*q.* Omnibus Diplomatic Security and Antiterrorism Act of 1986, 22 U.S.C. 4806 (Public Law 99-399)

*r.* Omnibus Consolidated Rescissions and Appropriations Act of 1996, 5 U.S.C. app. 11 note

*s.* Foreign Affairs Reform and Restructuring Act of 1998, 22 U.S.C. 6501 note (Division G of Public Law 105-277)

*t.* Federal Manager's Financial Integrity Act of 1982 (FMFIA) (Public Law 97-255)

*u.* 44 U.S.C., Chapter 31, Records Management by Federal Agencies (Federal Records Act)

*v.* 36 CFR, Chapter XII, Subchapter B, Part 1234, Electronic Records Management

## 5 FAM 1062.2 Executive Orders and Issuances

*(CT:IM-103; 01-23-2009)*

*a.* E.O. 13035, President's Information Technology Advisory Committee February 11, 1997 *b.* E.O. 13011, Federal Information Technology, July 16, 1996

*c.* E.O. 12472, Assignment of National Security and Emergency Preparedness Telecommunication Functions, April 3, 1984

*d.* E.O. 12656, Assignment of Emergency Preparedness Responsibilities

*e.* E.O. 12958, (Amended 13092) Classified National Security Information, April 17, 1995

*f.* PDD 62, Protection Against Unconventional Threats to the Homeland and Americans Overseas (Summary)

*g.* PDD 67, Enduring Constitutional Government and Continuity of Government Operations

*h.* Homeland Security Presidential Directive No. 7, December 2003

*i.* National Security Decision Directive 211 (Partially Classified)

## 5 FAM 1062.3 Guidelines and Standards

*(CT:IM-103; 01-23-2009)*

*a.* OMB Memorandum M-00-10, OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act, April 25, 2000

*b.* OMB Memorandum M-00-15, OMB Guidance on Implementing the Electronic Signatures in Global and National Commerce Act, September 25, 2000

*c.* OMB Memorandum M-02-09, OMB Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones

*d.* Circular A-130, OMB White House Office of Management and Budget, Appendix III, February 8, 1996 as amended

*e.* Circular A-11, OMB Part 6: Preparation and Submission of Strategic Plans, Annual Performance Plans, and Annual Program Performance Reports

*f.* OMB Circular A-76, Performance of Commercial Activities, 5/23/1996 (Revised 5/29/2003)

*g.* OMB Memorandum M-96-22, Implementation of the Government Performance and Results Act of 1993, 4/11/1996

*h.* OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, 12/16/2003

*i.* Federal Preparedness Circular 65, Federal Executive Branch Continuity of Operations

*j.* National Plan for Information Systems Protection, President’s Management Agenda *k.* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 Rev 1: Guide for Developing Security Plans for Information Technology Systems, February 2007

*l.* NIST SP 800-26: Security Self-Assessment Guide for IT Systems, November 2001

*m.* NIST SP 800-30: Risk Management Guide for Information Technology Systems, July 2002

*n.* NIST SP 800-34: Contingency Planning Guide for IT Systems, June 2002

*o.* NIST SP 800-35: Guide to Information Technology Security Services, October 2003

*p.* NIST SP 800-37: Guidelines for the Security Certification and Accreditation (C&A) of Federal Information Technology Systems, May 2004

*q.* NIST SP 800-53: Recommended Security Controls for Federal Information Systems, February 2005

*r.* NIST SP 800-55: Security Metrics Guide for Information Technology Systems, July 2003

*s.* NIST SP 800-59: Guideline for Identifying an Information System as a National Security System, August 2003

*t.* NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories, September 2004 Volume 1

*u.* NIST SP 800-64: Security Considerations in the Information System Development Life Cycle, October 2003

*v.* NIST SP 800-65: Integrating Security into the Capital Planning and Investment Control Process, January 2005

*w.* NIST SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, March 2005

*x.* Federal Information Processing Standard 199, (FIPS 199) Standards for Security Categorization of Federal Information and Information Systems, February 2004

*y.* Federal Information Processing Standard 200, (FIPS 200) Minimum Security Requirements for Federal Information and Information Systems, March 2007

# 5 FAM 1063 INFORMATION ASSURANCE OFFICE FUNCTIONS

## 5 FAM 1063.1 Organization and Administration

*(CT:IM-82; 02-22-2007)*

The CISO must develop and maintain a Department-wide information security program consisting of management, tactical, and operational program elements indicating their respective ownership and program managers in order to comply with Federal Information Security Management Act (FISMA) requirements.

## 5 FAM 1063.2 Program Management

*(CT:IM-82; 02-22-2007)*

a. Under direction of the CISO, the Information Assurance Office’s (IRM/IA’s) program management personnel internally coordinate strategic planning, including the Department-wide Information Security Program Plan and the Information Security Architecture.

b. IRM/IA’s program management personnel organize the production of program documentation covering various information security, information assurance, and risk management processes.

## 5 FAM 1063.3 Management Analysis

*(CT:IM-82; 02-22-2007)*

a. IRM/IA management analysis personnel:

   (1) Formulate and submit recommendations to the CISO on Department strategic and operational planning priorities, including funding for information security and information assurance activities;

   (2) Maintain working relationships with all bureaus; and

   (3) Support implementation of Earned Value Management (EVM) processes within IRM/IA in compliance with the Department’s guidelines.

b. The management analysis personnel foster universal compliance with security requirements in contracting, acquisitions, and capital planning.

## 5 FAM 1063.4 Planning

*(CT:IM-82; 02-22-2007)*

a. Planning encompasses evaluations of the security provisions of information system investments for the E-Gov Program Board via the E-Gov Program Office (IRM/BPC/EAP/PL). See 5 FAM 914.

b. IRM/IA planning personnel assist program managers in preparing investment proposals through the use of two publications:

   (1) The Department's Information Technology (IT) Cost Estimation Guide, managed by IRM/IA, is used to formulate budgets and costs for security activities; and

   (2) The e-CPIC Security and Privacy Guide. The Capital Planning and Investment Control (CPIC) process is described in detail in 5 FAM 1040.

## 5 FAM 1063.5 Reporting

*(CT:IM-82; 02-22-2007)*

a. The CISO oversees the collection, correlation, and drafting of the FISMA annual assessment and quarterly updates for submittal to Congress and the Office of Management and Budget (OMB). These evaluations address the adequacy and effectiveness of the Department's information security policies, procedures, and practices, and their compliance with Federal mandates.

b. In compliance with FISMA, managers of information systems projects and programs must develop and implement information security performance measures and include these measures in their project plans. Contact the IRM/IA for guidance on program outputs and outcome measurements.

c. Quarterly, systems owners must review and update their plan-of-action-and-milestones (POA&M) tool:

   (1) POA&M reports must list residual risks and remediation efforts associated with the information systems under their control (see 5 FAM 814 for definition of system owner);

   (2) Failure to submit quarterly POA&M updates may result in loss of funding and could lead to loss of accreditation and termination of the program.

d. IRM/IA publications issued to assist program managers and system owners with generating a POA&M include:

   (1) The State Automated FISMA Reporting Environment (SAFIRE) Guide;

   (2) The Information Technology Cost Estimation Guide; and

   (3) The POA&M Process Guidance documents. IRM/IA develops and tracks the Department-level POA&M.

   (See the IRM/IA Web site for more information on the current application and guides.)

# 5 FAM 1064 SECURITY PROGRAM

## 5 FAM 1064.1 Information Security Program Plan

*(CT:IM-82; 02-22-2007)*

a. IRM/IA develops and maintains the Department's Information Security Program Plan (ISPP) (see IRM/IA Web site for the ISPP).

b. The information security performance measures IRM/IA develops must gauge accurately the Department's operational information security functions that will be reported to the Office of Management and Budget (OMB).

c. System owners and program managers must incorporate these information security performance measures into their program plans. (Contact IRM/IA for more information on performance measures.)

## 5 FAM 1064.2 Contingency Planning and Continuity of Operations

*(CT:IM-82; 02-22-2007)*

a. System owners and non-Department entities (i.e., organizations, individuals, or other agencies) that process Federal information on behalf of the Department must:

(1) Develop and maintain contingency plans for the major applications and general support systems under their control that process, store, or transmit Federal information;

(2) Use the Department's Contingency Plan (CP) template to prepare the contingency plan (see the Contingency Plan template available on the Information Assurance IRM/IA Web site);

(3) For purposes of inspection, retain copies of the contingency plan and test results for the life of the system;

(4) Update and test the contingency plan when the major application or general support system has undergone a major change to its operational baseline configuration; and

(5) For moderate and high impact systems, test the contingency plan at least annually to verify the entities' ability to recover and/or restore the application or system to operation in the event of a system or application failure.

b. IRM/IA will assess system security, contingency planning, and continuity of operations efforts, and assist system owners in correcting deficiencies.

## 5 FAM 1064.3 Documentation

*(CT:IM-82; 02-22-2007)*

a. In support of the FISMA compliance requirements, IRM/IA maintains an active library of systems authorization and risk management documentation, which is used to support analysis of changes to approved operational baselines, re-evaluation of accepted risk, and as the reference source for entries in the Department's automated POA&M management tool.

b. As part of the Systems Authorization Process, system owners must provide current copies of their system's contingency and system security plan to the certification team prior to requesting authorization of the system:

   (1) The System Security Plan (SSP) and the Department's Contingency Plan (CP) must be up-to-date with the system's current configuration and system recovery requirements;

   (2) These documents must reflect the actual state of the security controls, including any modifications or changes made during the tailoring process of the security control baseline.

c. The executive director (or equivalent level) for a bureau-sponsored non-Department entity must ensure that current copies of the non-Department entity's system contingency plan, system security plan, and independent certifiers report are provided to IRM/IA.

d. IRM/IA documentation personnel ensure that only current and IRM/IA-approved copies of all guides and reference documents and templates are posted and available on the IRM/IA Web site.

# 5 FAM 1065 RISK MANAGEMENT

## 5 FAM 1065.1 Certification

### 5 FAM 1065.1-1 Information System Security Control Assessment

*(CT:IM-103; 01-23-2009)*

a. Designated certification personnel must perform security control assessments of all FISMA reportable Department systems except those systems designated as sensitive compartmented information (SCI) (see 1 FAM 271 *(4).*)

b. The certifier (information security auditor) must provide the Location-

Specific System FISMA Compliance Report to IRM/IA (risk analysis personnel) within two weeks of completing the Location-Specific System FISMA compliance visit.

c. The system owner must perform an annual security control self-assessment using the automated plan-of-action-and-milestones (POA&M) reporting tool.

d. Security control assessment must be performed in accordance with FISMA guidance. (Contact IRM/IA for current Department guidelines.)

e. Unclassified non-National Security Systems (non-NSS) with medium or high security categorization impact levels must be independently certified. (See NIST SP 800-53.)

f. Classified and unclassified NSS must be independently certified. (See 40 U.S.C. 11103 for definition of NSS.)

## 5 FAM 1065.1-2 General Certification Requirements

*(CT:IM-103; 01-23-2009)*

a. An independent certifier must perform the independent certification, as defined in this subchapter (see 5 FAM 1065.1-4).

b. Bureaus requiring independent certification of their systems may use independent certification resources available from independently contracted qualified vendors, or from internal bureau-independent certifiers.

c. Vendors selected to perform independent certification of a medium or high security categorization impact level system must be fully qualified in accordance with Department policy and any specific requirements defined in the contract (e.g., Form DD-254, Contract Security *Classification* Specification, or contract modification).

d. The Information Assurance Office (IRM/IA) must ensure that independent certification resources are compliant with 5 FAM 1065.1-2 a prior to the start of system certification.

e. IRM/IA must provide oversight of the independent audit function by performing selected random quality assurance evaluations of independent certification reports to ensure full compliance with Department requirements.

## 5 FAM 1065.1-3 Certification Requirements For Low Impact Systems

*(CT:IM-82; 02-22-2007)*

a. A system owner is authorized to perform certification of low impact systems.

b. All certification results of low-impact systems must be forwarded to Information Assurances Office IRM/IA for validation within 10 business days of completion of certification.

c. Failure to provide IRM/IA with the certification results of low-impact systems may invalidate the system’s certification.

## 5 FAM 1065.1-4 Criteria for Independent Certification

*(CT:IM-82; 02-22-2007)*

a. Assessor independence implies that the certification agent (or certification team), whether obtained from within the organization or external to the organization, is not involved with the information system’s development, implementation, or operation. (See NIST SP 800-53.)

b. A U.S. Government-affiliated internal certification organization can be presumed to be free from organizational impairments to independence when reporting internally to management only if the head of the audit organization meets all of the following criteria:

(1) Accountable to the head or deputy head of the U.S. Government entity;

(2) Required to report the results of the audit organization’s work to the head or deputy head of the U.S. Government entity; and

(3) Located organizationally outside the staff or line management function of the system owner. (Reference, Government Auditing Standards, 2003 Revision, GAO-03-673G, June 2003, Page 25.)

## 5 FAM 1065.1-5 Penetration Testing

*(CT:IM-82; 02-22-2007)*

a. The Bureau of Diplomatic Security’s Cyber Threat Analysis Division (DS/CS/CTA) executes penetration testing of the Department’s networks. The CISO provides oversight to this internal and external penetration testing of selected general support systems (GSSs) and designated critical applications in support of the systems authorization program and, as general information, security performance program (e.g., financial applications, medical applications). In addition, the CISO:

(1) Coordinates the schedule for systems to be tested with the Office of Computer Security (DS/SI/CS); and

(2) Coordinates with Office of the Senior Coordinator for Security Infrastructure (DS/SI), the GSSs, and designated applications selected for penetration testing, and established schedule for the

penetration tests.

b. DS/SI must provide the results of all penetration testing of selected GSSs and designated applications to IRM/IA and the system owner within two weeks of test report completion.

### 5 FAM 1065.1-6 Unclassified Non-Department-Owned Systems Processing Federal Information

*(CT:IM-82; 02-22-2007)*

a. The executive director (or equivalent level) for a bureau-sponsored non-Department entity must ensure that the non-Department entity provides IRM/IA the results of an independent security control assessment of the non-Department-owned system that processes Federal information on behalf of the Department against the criteria provided by the Department as part of the certification and accreditation (C&A) process.

b. Executive directors (or equivalent level) for bureau-sponsored non-Department entities must ensure that the annual security control self-assessment required by the Federal Information Security Management Act (FISMA) for non-Department-owned systems that process Federal information on behalf of the Department is completed, and the results are forwarded to the bureau.

c. The annual self-assessment must be performed in accordance with the Plan-of-Action-and-Milestones (POA&M) Process Guide. (See the IRM/IA Web site for current guide.)

d. The executive director (or equivalent level) for bureau-sponsored non-Department entities must ensure the inclusion of the results of the annual security control self-assessment in the bureau's POA&M.

## 5 FAM 1065.2 Risk Analysis

*(CT:IM-82; 02-22-2007)*

a. Risk analysis/risk management personnel:

(1) Balance the tangible and intangible cost to the Department of applying security safeguards against the value of information and the associated information system; and

(2) Follow a defined methodology recommended by the National Institute of Standards and Technology (NIST) in Special Publication 800-30.

b. IRM/IA risk management personnel perform risk analysis of Department and non-Department systems, which process Federal information on behalf of the Department, in support of the Systems Authorization process and FISMA reporting requirements.

## 5 FAM 1065.3 Special Assessments

*(CT:IM-82; 02-22-2007)*

a. IRM/IA special assessments personnel:

(1) Generate risk assessments and estimates to prepare recommendations for decisions on nonstandard requests, such as exceptions to policy, deviations from standards, and changes to policy that affect the operational information risk profile of the Department; and

(2) Prepare a risk estimate in lieu of an assessment when insufficient vulnerability data exists to support a full assessment.

b. For detailed information on special assessments, contact the IRM/IA's risk analysis staff.

### 5 FAM 1065.3-1 Requests for Interagency and Non-Department Connectivity

*(CT:IM-103; 01-23-2009)*

a. IRM/IA special assessments personnel evaluate requests from bureaus requiring other agencies and non-Department entities to connect to Department information systems.

b. Connectivity requests must include:

(1) A Signed Memorandum of Agreement or Understanding (MOA/MOU);

(2) An Interconnection Security Agreement (ISA); and

(3) For commercial contractors and consultants with contractual relations with the Department, Form DD-254, Contract Security Classification Specification, or other document containing contract security requirements language specifying all information contained in a connectivity MOA/MOU and ISA.

c. Contact IRM/IA special assessment personnel for further assistance.

d. IRM/IA special assessments personnel must develop an assessment of risk to ensure that the requested connections meet the standards and guidelines set forth in the NIST SP 800-47, and Department information security policies.

### 5 FAM 1065.3-2 Requests for Waivers, Exceptions, and Deviations

*(CT:IM-103;   01-23-2009)*

a. System owners must submit to IRM/IA and to DS/SI/CS requests for waivers *of*, exceptions to, or deviations from required information security controls or processes. The request must outline:

   (1) Why the controls cannot be maintained, including the resource implications;

   (2) Why the actions are required at the time of the request; and

   (3) How long it will be until compliance can be achieved.

b. Requests for waivers of, exceptions to, or deviations from policies, standards, or approved processes, which affect information security specified in 12 FAM 600 and 5 FAM or other applicable Federal mandates, require a justification relative to operational resource implications.

c. DS/SI/CS personnel must perform a security vulnerability assessment outlining the technical ramifications of the request.

d. DS/SI/CS assessment results, any recommendations for compensating controls, and recommendation for approval or disapproval must be provided to the CISO upon completion.

e. IRM/IA special assessments personnel must develop an impact assessment, or estimate of the risk, and based on the impact assessment results, submit recommendations for approving or disproving the request to the CISO.

f. The CISO must send an official memorandum (domestically) or telegram (abroad) to the requesting system owner detailing the final decision (approval or disapproval) on the waiver, exception*,* or deviation request:

   (1) If the CISO approves the request for implementation domestically, the system owner must:

      (a) Within 30 days, endorse the memorandum, in writing, acknowledging his or her understanding and acceptance of the decision and any terms/conditions; and

      (b) Make a copy of the endorsed memorandum for his or her record, and return the original memorandum with endorsement to the CISO*.*

   (2) If the CISO approves the request for implementation abroad, the system owner must:

      (a) Send a telegram to the CISO acknowledging acceptance of the decision and any terms/conditions; and

      (b) For future reference and inspection, ensure copies of all documents related to the request are on file at post*.*

(3) In both subparagraphs f(1) and f(2) of this section, the system owner must not implement the requested change until he or she accepts the terms and/or conditions of the approved request.

(4) If the request is disapproved, the system owner must not, in any case, implement the requested change.

(5) IRM/IA must provide a copy of the final decision memo to DS/SI/CS.

g. DS must coordinate with the CISO all waivers, deviations, and exceptions to the Overseas Security Policy Board (OSPB) standards (12 FAH-6) for Department of State systems. (See 1 FAM 266.2 *(10)*.)

h. System owners or executive directors (or equivalent level) for bureau-sponsored non-Department entities must submit to the Information Technology Change Control Board (IT CCB) all requests for changes to the Department's security configuration guides produced by the Global Support Division (DS/CS/ETPA). (See IT CCB's Web site for further information.)

i. The provisions of 5 FAM 1065.3-2 do not apply to Information Assurance (IA) and IA-enabled products employed with or in classified information processing systems as defined in 5 FAM 913. These products require a Deferred Compliance Authorization (DCA). (See 5 FAM 915.15-4.)

j. All Dedicated Internet Network waiver requests are processed through the ITCCB. (See 5 FAM 874.2.)

## 5 FAM 1065.4 Systems Accreditation

*(CT:IM-103; 01-23-2009)*

a. To be compliant with OMB Circular A-130, Management of Federal Information Resources*,* Federal agencies must:

(1) Plan for security;

(2) Ensure appropriate officials are assigned security responsibility; and

(3) Authorize system processing prior to operations and periodically thereafter.

b. Systems authorization of all FISMA reportable Department systems must be performed. IRM/IA developed the Systems Authorization Process to comply with this requirement.

c. All FISMA reportable information systems within the Department must complete the Department's System Authorization Process and be authorized by a Designated Approving Authority (DAA) before being permitted to operate. *(*See 1 FAM 271.2 (7).*)*

d. As part of the Systems Authorization Process, Department system owners responsible for Department information systems, including those responsible for non-Department entities (e.g., contractors, vendors), must perform security categorization of the Federal information they process on behalf of the Department. See the Department of State Acquisition Regulation (DOSAR) for further guidance on non-Department entities.

e. For unclassified systems, system owners and executive directors (or equivalent level) for bureau-sponsored non-Department entities must accomplish the categorization of the information and information system, as defined in Federal Information Processing Standards (FIPS) 199, during the Information Technology Application Baseline (ITAB) registration process. Executive directors (or equivalent level) for bureau-sponsored non-Department entities are responsible for registering non-Department systems in the ITAB. The only information categories evaluated for non-Department entities are those that process Federal information on behalf of the Department.

f. The Department system owner must determine a classified system’s impact level during the ITAB registration process. Executive directors (or equivalent level) for bureau-sponsored non-Department entities are responsible for registering non-Department systems in the ITAB.

g. The potential impact to the Department in terms of loss of confidentiality, integrity, and availability of information on an unclassified information system is defined in FIPS 199 and is tailored to Department needs and agreed to by the e-Gov advisory board:

(1) **LOW** - if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on Department operations, Department assets, or individuals;

(2) **MODERATE** - if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on Department operations, Department assets, or individuals; and

(3) **HIGH** - if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on Department operations, Department assets, or individuals.

h. System owners must establish the baseline security control configuration for information systems under their control. The baseline security control configuration is based on the potential impact level determined by the security categorization completed during the ITAB registration process. The baseline configuration consists of the minimum information system security controls required under FISMA for information systems. (See IRM/IA Web site for the most current security control guidelines.)

i. Using the SSP system owners must document the information system security controls identified in the system baseline and verify each as planned, implemented, partially implemented, or not applicable. (See IRM/IA Web site for the most current template.)

j. Mandatory security controls must be implemented without exception.

k. System owners may enhance mandatory security controls without waiver or deviation (without changing the non-major application designation if the application has been identified as a non-major application). The SSP must document the enhancements, and these enhancements must be reported in the system's POA&M, if these enhancements affect a material weakness or system vulnerability.

l. To strengthen its security posture without a waiver, exception, or deviation, system owners may add information security controls that are not mandatory for the selected security control baseline. These additional controls will not change a non-major application designation if the application has been identified as a non-major application.

m. System owners must report the status of implementation and/or remediation of identified deficiencies of the information system security controls in the system's POA&M.

## 5 FAM 1065.4-1 Department Information Systems

*(CT:IM-103; 01-23-2009)*

a. IRM/IA must ensure systems authorization is performed on all Department information systems. (See 1 FAM 266.1 for SCI systems.)

b. IRM/IA must ensure system authorization is performed in accordance with the approved Department System Authorization Process Guide available on the IRM/IA Web site.

c. The Bureau of Diplomatic Security's Evaluation and Verification Program, in compliance with the FISMA reporting requirements, must evaluate and validate location-specific system security controls. Location-specific system security controls must be verified yearly as well as part of the systems authorization process. Results of these evaluations are reported to IRM/IA and must be included in the system's POA&M. (See 1 FAM 266.2-4.)

d. Security control baselines for Department systems must be established in accordance with Department guidelines using the impact level established during the Information Technology Application Baseline (ITAB) registration process and documented in the system's SSP prior to commencement of certification. (See IRM/IA Web site for the most current security control guidelines.)

e. Systems owners are responsible for all funding required to perform C&A of their systems.

## 5 FAM 1065.4-2 Unclassified Non-Department-Owned Systems Processing Federal Information

*(CT:IM-82; 02-22-2007)*

a. The executive director (or equivalent level) for bureau-sponsored non-Department entities processing Federal information on behalf of the Department must register these systems in the Department's ITAB.

b. Security control baselines for non-Department systems must be established in accordance with Department guidelines, using the impact level established during the ITAB registration process, the requisite contract security requirements, and documented in the system's SSP prior to commencement of certification. The non-Department entities must document the baseline in the system's SSP, using the SSP template from NIST Special Publication 800-18. (See IRM/IA Web site for the most current security control guidelines.)

c. Contingency plans are required for non-Department-owned systems that process Federal information on behalf of the Department. The non-Department entities must develop the contingency plans in accordance with NIST Special Publication 800-34, and ensure they are fully tested, at least annually. The executive director (or equivalent level) for bureau-sponsored non-Department entities must ensure that the contingency plans have been tested and the results reported to IRM/IA.

d. The Department's Systems Authorization Process requires that a risk analysis be performed on non-Department-owned systems processing Federal information on behalf of the Department.

e. The executive director (or equivalent level) for a bureau-sponsored non-Department entity responsible for the Federal information being processed by the non-Department entity on behalf of the Department must report in the POA&M the status of remediation of identified deficiencies of information system security controls contained in the baseline, as documented in the SSP.

f. System Authorization of unclassified non-Department-owned systems must be performed in accordance with the Department's System Authorization Process.

g. The executive director (or equivalent level) for bureaus sponsoring the non-Department entity processing or storing Federal information on behalf of the Department must ensure the yearly self-assessments required for FISMA reporting are completed and the results provided to IRM/IA. See POA&M Process Guide.

## 5 FAM 1065.4-3 Classified Non-Department-Owned Systems Processing Federal Information

*(CT:IM-103;   01-23-2009)*

a. On behalf of the Department, the Cognizant Security Agency (CSA), in coordination with the Bureau of Diplomatic Security’s Industrial Security Division (DS/IS/IND), performs certification and accreditation (C&A) of classified non-Department-owned systems operated by commercial firms and consultants under contractual agreement with the Department. (See National Industrial Security Program Operating Manual (NISPOM) and 12 FAM 570.)

b. Upon completion of C&A, DS/IS/IND must provide DS for sensitive compartmented information (SCI) systems and IRM/IA for all other systems with a copy of the accreditation package, as approved by the Department’s designated approving authority (DAA). (See 1 FAM 271.2 e(7).)

c. DS/IS/IND must conduct the yearly assessments required for FISMA reporting for those commercial firms and consultants under contractual agreement processing classified information on behalf of the Department. DS/IS/IND must provide the results of these assessments to IRM/IA and the executive director (or equivalent level) for bureau-sponsoring non-Department entities for inclusion into the sponsoring bureau’s POA&M.

d. The sponsoring bureau must ensure the yearly self-assessments required for FISMA reporting for non-Department entities processing information on behalf of the Department without a contractual agreement with the Department (i.e., State, local government agencies, etc.) are conducted. The sponsoring bureau must provide the results of these self-assessments to IRM/IA and the executive director (or equivalent level) for bureau-sponsoring non-Department entities for inclusion into the sponsoring bureau’s POA&M.

## 5 FAM 1065.5 Vulnerability Scanning

*(CT:IM-82;   02-22-2007)*

a. Using appropriate techniques and IT CCB-approved vulnerability scanning tools, DS/SI/CS, the Evaluation and Verification Program personnel, must scan for vulnerabilities in the information system periodically, as well as when significant new vulnerabilities affecting the system are identified and reported.

b. Vulnerability scanning tools should include the capability to readily update the list of vulnerabilities scanned.

c. DS/SI/CS, the Evaluation and Verification Program personnel, must update the list of information system vulnerabilities when discovered.

d. Vulnerability scanning procedures must include steps to ensure adequate scan coverage and include both vulnerabilities checked and information system components scanned.

e. DS/SI/CS must provide the results of periodic scanning to the CISO and the system owner.

# 5 FAM 1066 INFORMATION SECURITY POLICY AND PROCESS

## 5 FAM 1066.1 Policy

*(CT:IM-103; 01-23-2009)*

a. In support of information security policy and process, IRM/IA policy personnel and staff:

(1) Develop and maintain the information security policy framework;

(2) Collect, identify, and document information security requirements for the development of information security policy;

(3) Draft information assurance policy and procedures for 5 FAM 1060;

(4) Maintain liaison with the enterprise information systems security management (EISSM) personnel to determine if existing policies provide adequate information security or if additions or revisions are necessary;

(5) Issue interim guidance and emergency policy, in conjunction with DS/CS/ETPA, to assist field personnel in maintaining adequate information security. (**NOTE**: Interim guidance or emergency policy is only issued when time is needed to update and clear a policy or procedure in the FAM or FAH (see 2 FAM 1115.2 for policy issuance details));

(6) *A*re responsible*, as subject matter experts (SMEs) for content,* for change control for 5 FAM 1060, and submit these changes to the Information Resources Policy and Regulations Office (IRM/BPC/PRG) for processing and clearance;

(7) Coordinate internal Department policy document reviews requested from NIST concerning national information security issues;

(8) Assess the impact of new legislation on the Department's security standards and policies. Upon completion of the assessment, the CISO must provide direction in writing to the Deputy Chief Information Officer for Business Planning and Customer Service/Chief Knowledge Officer (IRM/BPC) and the Senior Coordinator for Security Infrastructure (DS/SI) to revise their respective FAM/FAH sections to ensure compliance. IRM/IA should

submit all FAM/FAH changes to IRM/BPC/PRG for processing; and

(9) Perform other appropriate and authorized tasks as designated by the CISO or CIO.

b. IRM/IA policy personnel and special assessment personnel jointly analyze waiver, deviation, and exception request trends to identify policy revision requirements.

c. Deputy Chief Information Officer For Operations/Chief Technology Officer (IRM/OPS) must advise IRM/IA of the development of all cyber security procedures for operational elements.

d. DS/CS/ETPA maintains and updates the Department's information security policies, in conjunction with IRM/IA and IRM/BPC/PRG.

## 5 FAM 1066.2 Process

*(CT:IM-82; 02-22-2007)*

a. IRM/IA policy personnel must assist program management personnel in defining and documenting IRM/IA operational processes, and coordinate and develop all internal IRM/IA process guides.

b. IRM/IA documentation personnel must maintain an archive of final approved copies of all IRM/IA process guides.

# 5 FAM 1067 ENTERPRISE INFORMATION SYSTEMS SECURITY MANAGEMENT (EISSM) AND TRAINING

## 5 FAM 1067.1 Enterprise Information Systems Security Management (EISSM)

*(CT:IM-82; 02-22-2007)*

a. IRM/IA enterprise information system security management (EISSM) personnel manage the Department's Information System Security Officer (ISSO) Program. EISSM personnel:

(1) Provide liaison and technical assistance to the ISSOs in performing ISSO duties;

(2) Ensure ISSO staffing is commensurate with information assurance requirements. Specific ISSO duties and responsibilities are available on the IRM/IA Web site;

(3) Maintain the on-line ISSO library and ISSO ListServ as a resource

to assist ISSOs in performing their duties; and

(4) Assist system owners in becoming compliant with Federal and Department information system security requirements.

b. EISSM and risk personnel are active members of the Department's Firewall Advisory Board (FAB). (See 5 FAM 115.8-1 for details on the FAB.)

c. EISSM personnel serve as the IRM/IA point-of-contact with the Department's Computer Incident Response Team (CIRT), the Foreign Service Institute (FSI), and the Bureau of Diplomatic Security Training Center.

d. Personnel assigned ISSO responsibilities must be tenured (if a Foreign Service employee), Top Secret-cleared, direct-hire employees having the necessary management experience and training with the Department's automated information systems (AISs). Requests for exception to this requirement, including contractual personnel, must be fully justified and submitted to the CISO.

## 5 FAM 1067.2 Awareness, Training, Education and Professionalism (ATEP)

### 5 FAM 1067.2-1 General

*(CT:IM-82; 02-22-2007)*

a. The CISO must implement information security awareness training to inform Department personnel and non-Department entities of the security risks inherent in operating the Department's automated information systems.

b. Security awareness training must inform employees and non-Department entities of their responsibilities in complying with Department policies and procedures designed to reduce risk to Department information systems, as well as penalties for noncompliance. (See 44 U.S.C. 3544.)

### 5 FAM 1067.2-2 Training and Education Program

*(CT:IM-103; 01-23-2009)*

*a. IRM/IA, in conjunction with the Awareness, Training, Education and Professionalism (ATEP) Working Group, oversees the planning and content of all security awareness training, role-based training, education, and professional programs. Membership of the ATEP includes IRM/IA, DS/SI/CS, the Security Engineering and Computer Security Training Division (DS/TPS/SECD), the Foreign Service Institute School of Applied Information Technology (NFATC/FSI/SAIT), and the Office of the*

*Inspector General (OIG).*

b. *Training programs must include annual awareness training for all system users.*

c. *Training programs must include specific role-based security training for identified Department personnel with significant information security responsibilities.* The Department of State IA Training *plan identifies the training requirements. (See the Security Awareness, Training, and Education policy contained in 5 FAM 845.)*

## 5 FAM 1067.2-3 Responsibilities

*(CT:IM-103; 01-23-2009)*

a. *The CISO is responsible for approving the cyber security awareness training, role-based training, education, and professional programs.*

b. *DS/SI/CS is responsible for developing and delivering the cyber security awareness training program. (See 5 FAM 845.)*

c. *DS/TPS/SECD is responsible for development and delivery of role-based cyber security training. (See 5 FAM 845.)*

d. *NFATC/FSI/SAIT is responsible for including cyber security information in technical training and tradecraft courses.*

# 5 FAM 1067.3 Patch Management Compliance Program

*(CT:IM-103; 01-23-2009)*

a. *IRM/IA (i.e., enterprise information system security management (EISSM) personnel) is responsible for managing and implementing the Patch Management Compliance Program.*

b. *Patch management compliance is defined as:*

(1) *For critical patches: achieving and maintaining a patch installation rate of 100%, as designated by the Enterprise Network Management Office (IRM/OPS/ENM);*

(2) *For all workstations and servers on OpenNet and ClassNet: achieving and maintaining a patch installation rate 90% of all patches within 15 days after patch release.*

c. *Sites not in compliance with this program risk sanctions from the CIO. (See 5 FAM 866.)*

d. *To mitigate compatibility issues with local applications, personnel responsible for sites should establish a representative system of all local applications for testing purposes.*

*e. IRM/IA will work with IRM/OPS/ENM and personnel responsible for sites to determine if there are circumstances that preclude a site from reaching an acceptable level.*

*f. IRM/IA must notify stakeholders, including the CIO, CISO, DS/SI, Regional Information Management Center (RIMC) Directors, ISSOs, post information management officers (IMOs), and system owners quarterly of sites with satisfactory or unsatisfactory compliance status with official OpenNet and ClassNet patch installation implementation.*

*g. Personnel responsible for sites must document concerns of sites that have issues related to implementing patches and report those concerns to the IRM InfoCenter.*

# 5 FAM 1068 ADVISING

## 5 FAM 1068.1 Technical Consultation

*(CT:IM-82; 02-22-2007)*

a. IRM/IA provides technical information security assistance to the Information Technology Change Control Board (IT CCB), as the system authorization security reviewer for all applications except those for SCI systems.

b. DS/SI coordinates with the CISO the Department’s position on computer security issues brought to the Overseas Security Policy Board (OSPB).

c. IRM/IA assists the Bureau of Resource Management (RM) with the development and maintenance of the Department’s Critical Infrastructure Protection Plan (CIPP) to protect the Department’s critical information system assets and infrastructure.

d. IRM/IA provides technical assistance to the Enterprise Architecture Division (IRM/BPC/EAP/EA) in evaluating modifications to the Department’s information security architecture.

## 5 FAM 1068.2 Analyses of New Information Technologies

*(CT:IM-82; 02-22-2007)*

a. IRM/IA special assessments personnel must conduct an initial risk estimate associated with each planned new technology pilot after completion of its concept of operations (ConOps) plan and prior to implementing the new technology as a pilot or test program.

b. The system owner must register all new technology pilots in the ITAB, and plan for conducting the system authorization process prior to the new technology's production operational deployment. This planning is vital to avoid a period of non-operation between the pilot or test and operational deployment as the systems authorization process completes.

## 5 FAM 1068.3 Liaison

*(CT:IM-82;   02-22-2007)*

a. IRM/IA liaison personnel represent the Department:

(1) On interagency and intra-agency boards, working groups, and councils with charters related to information security and critical infrastructure protection for non-SCI systems;

(2) With the Office of Management and Budget (OMB) regarding cyber-security issues;

(3) With responses to Congressional inquiries in coordination with the bureau of Legislative Affairs (H) on cyber-security issues; and

(4) With the Office of Inspector General (OIG) on cyber-security issues.

b. IRM/IA advocate personnel must be the liaison between IRM/IA and all others, including system owners and non-Department entities regarding all system authorization or assessment matters.

c. IRM/IA reporting personnel chair the Cyber Security Budget Working Group with RM, IRM/OPS, and the Office of the Executive Director of the Bureau of Diplomatic Security (DS/EX) to establish FISMA-required cyber-security budget reporting processes and data collection requirements.

# 5 FAM 1069 UNASSIGNED