5 FAH-11 H-200 CERTIFICATION (INFORMATION SECURITY AUDIT)

5 FAH-11 H-210 GENERAL

(CT:IM-4;   06-13-2007)
(Office of Origin: IRM/IA)

5 FAH-11 H-211 INTRODUCTION

5 FAH-11 H-211.1 Purpose

(CT:IM-4;   06-13-2007)

This subchapter establishes a uniform approach to systems certification from an information security audit perspective. It incorporates many of the certification procedures developed from past practices and in use by the Bureau of Information Resource Management, Office of Information Assurance (IRM/IA).

5 FAH-11 H-211.2 Scope

(CT:IM-4;   06-13-2007)

a. This subchapter implements the policy in 5_FAM 1060 (Information Assurance Management) and supplements guidance in various National Institute of Standards and Technology (NIST) publications, Office of Management and Budget (OMB) direction, Foreign Affairs Manual (FAM), General Accounting Office (GAO) publications, and Congressional and Executive Orders.

b. This subchapter excludes certification of secure compartmented information (SCI) systems. The Office Director of the Office of Information Security (DS/SI/IS) is the Designated Approving Authority (DAA) for SCI systems (see 1 FAM 266.1).

c. Individuals performing or participating in certifying a system, whether a Department or non-Department system, must comply with the certification process in this document to complete certification.

d. IRM/IA is responsible for the content of this subchapter. Send questions to IRM/IA at informationassurance@state.gov.

5 FAH-11 H-211.3 Objectives

(CT:IM-4; 06-13-2007)

The following objectives are vital to improving the effectiveness of information security through system certification:

(1) Ensure that certification procedures fully assess system security controls and other factors (e.g., accuracy of the documentation);

(2) Apply the requirements for systems certification as defined in this sub-chapter to the Systems Authorization Process (contact IRM/IA for further guidance);

(3) Ensure the effective implementation of the Department's information security program plan (ISPP);

(4) Ensure that Federal Information Security Management Act of 2002 (FISMA) requirements mandated for system certification and accreditation (C&A) are met;

(5) Ensure compliance with regulations and standards aimed at protecting sensitive consumer data;

(6) Ensure requirements and procedures for conducting independent certification of selected systems are followed; and

(7) Ensure systems certification requirements regarding general policy established in 5 FAM 1060 (Information Assurance Management) are implemented.

5 FAH-11 H-211.4 Authorities

(CT:IM-4; 06-13-2007)

The authorities that govern the process for certification of a Department information system are found in 5 FAM 1060 (Information Assurance Management).

5 FAH-11 H-211.5 Key Personnel

(CT:IM-4; 06-13-2007)

a. In the Department's sponsoring bureau, key personnel involved in system certification work closely with the certification analyst to ensure that Department and sponsored non-Department information systems are properly audited and that the information these systems process is protected from loss, damage, or compromise.

b. Key personnel of the sponsoring bureau form the systems authorization team assigned to certify and accredit a system under the Systems Authorization Process.

c. Key personnel assigned to domestic locations and facilities abroad support system certification as follows:

(1) Work with the certification analyst and others outside of the sponsoring organization to perform a system’s certification and analyze each system weakness and related criteria, including but not limited to:

(a) Condition identified;

(b) Cause of the weakness;

(c) Identified threats posed against the weakness; and

(d) Actual or potential impact the weakness represents.

(2) Participate in reviews and interviews during certification; and

(3) Provide review and input for meeting FAM and FAH requirements for certification of Department information systems.

d. Key personnel listed below have distinct roles for ensuring that systems meet certification requirements:

(1) Chief Information Officer (CIO): The CIO, as the Designated Approving Authority (DAA), ensures compliance with requirements set forth in FISMA's Title III, Information Security (see 44 U.S.C. 3544), and other federal guidelines and publications for unclassified and classified non-SCI systems. (See 5 FAH-11 H-211.2.)

(2) The Chief Information Security Officer (CISO), as the Authorizing Official's Designated Representative (AODR) ensures that the sponsoring bureau staff the key personnel and certification team positions and that these personnel meet the requirements of this subchapter and related policies, procedures, standards, and guidelines to complete system certification.

(3) The Information Systems Security Officer (ISSO) has responsibility for the information assurance of a system at every point in the life cycle.

(4) The System Owner:

(a) The Department system owner is the Senior Foreign Service (FS) or Senior Executive Service employee responsible for management and funding of the system. For non-Department systems, the system owner is the Senior Foreign Service employee, or the bureau executive director responsible for management and funding of the system. As set forth in this FAH, this employee is responsible for ensuring the system operates in accordance with the security controls outlined in its System Security Plan (SSP).

(b) The system owner begins the process and works with the system manager and certification team to coordinate scheduling and assigning resources to complete system certification. Assigned resources must be available and sufficient to support systems certification requirements and meet milestones established in the system's C&A work plan.

(c) During certification, the system owner must ensure the system's operational baseline remains stable, and that scheduled system modifications do not invalidate or interfere with the planned or ongoing Security Control Assessment (SCA).

(5) The System Manager:

(a) The system manager is primarily responsible for implementing a system's security configuration controls, and for remediating identified system weaknesses. For detailed information on Department security configuration documents, see the Office of Computer Security (DS/SI/CS) Web site.

(b) During certification, the system manager and ISSO work with the certification analyst and the systems authorization team to correct deficiencies identified in implementing a system's required security controls (i.e., operational, maintenance, and technical related).

(c) A system manager must:

(i) Create and maintain the system's security documentation as follows:

aa The SSP and the CP must be up-to-date and tested with the system's current configuration and system recovery requirements; and

bb All other security related documents must reflect the actual state of the security controls, including after the security assessment, and any modifications approved by the system owner that address the certification analyst's recommendations for corrective actions.

(ii) Perform a self-assessment if a system's authorization requires that one be performed;

(iii) Implement a system's security requirements to reduce risk to the operational infrastructure to an acceptable level; and

(iv) Inform the system owner of the status of the system's planned or implemented security controls, baseline configuration, and changes that may affect the system's security posture during certification.

(6) Certification Analyst:

(a) The certification analyst is responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome for meeting the system security requirements. The certification analyst also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system.

(b) To preserve the impartial and unbiased nature of the security certification, the lead certification analyst, coordinating certification of moderate and high impact unclassified systems and all classified systems, must be in a position that is independent from the persons directly responsible for the development of the information system and the day-to-day system operation. The certification analyst must also be independent of individuals responsible for correcting security deficiencies identified during security certification. Independence of the certification analyst is an important factor in assessing the credibility of the security assessment results, and ensuring the authorizing official receives the most objective information possible to make an informed, risk-based, accreditation decision. (See 5 FAM 1065.1-2 for the criteria for independent certifiers.)

5 FAH-11 H-212 CERTIFICATION AND ACCREDITATION REQUIREMENTS

(CT:IM-4;   06-13-2007)

a. Certification and accreditation (C&A) is the primary vehicle for managing risk for the Department's IT systems identified under OMB Circular A-130 requirements, and 5 FAM 1060, Information Assurance Management, policy.

(1) Certification is the comprehensive evaluation of the management,

operational, and technical security controls of an IT system to support the accreditation process. It establishes the extent to which a particular design and implementation of the system meets a set of specified security requirements.

(2) Accreditation is the formal decision by an accreditation body (or appropriate management authority) to authorize operation of an IT system and to accept the risk based on the implementation of the security controls.

b. C&A progresses under the Systems Authorization Process through four operational phases; however, only Phases I and II involve certification.

5 FAH-11 H-212.1 Certification Of Moderate Or High Impact Systems And Unclassified NSS

(CT:IM-4; 06-13-2007)

a. Unclassified non-National Security Systems (NSS) with moderate or high security categorization potential impact levels must be independently certified in accordance with 5 FAM 1060 requirements.

b. Find the definition of NIST in NIST SP 800-59 (Guideline for Identifying an Information System as a National Security System).

c. Independent certification must be performed under the guidance of an independent certifier as defined in 5 FAM 1060.

d. Bureaus requiring independent certification of a system may use independent certification resources available through:

(1) Internal government (or bureau) independent certifiers; or

(2) Certification services from qualified vendors outside of government or bureau influence.

NOTE: Vendors selected to perform independent certification of a moderate or high security categorization potential 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.)

5 FAH-11 H-212.2 Certification Of Low Impact Non-NSS Systems

(CT:IM-4; 06-13-2007)

a. The system owner can perform certification of low impact systems.

b. All certification results for low impact systems must be forwarded to IRM/IA for validation within 10 business days of completing certification.

c. Failure to provide IRM/IA with the certification results of low impact systems may invalidate the system's certification, which will prevent the system from completing Department requirements to receive DAA approval to operate.

5 FAH-11 H-212.3 Certification Process

(CT:IM-4; 06-13-2007)

a. For moderate and high impact systems requiring independent certification:

(1) The system owner forwards a System Authorization Request (SAR) to the Information Technology Change Control Board (IT CCB) requesting authorization of a system, indicating who will perform the independent certification;

(2) Upon receipt of the SAR, the IT CCB evaluates the system to assess if the system is ready to formally undergo C&A; and

(3) When the system or application is deemed ready to undergo certification, the system owner must coordinate certification requirements with the independent certifier.

b. For low impact, non NSS systems undergoing internal bureau certification, the system owner must:

(1) Forward a SAR to the IT CCB requesting authorization to operate for a system and indicates that the system is undergoing certification at the Bureau level; and

(2) Schedule certification, and identify and assign the internal bureau resources needed to certify the system.

c. All certification must be done using the certification checklists for low, moderate, and high impact systems. Certification checklists, along with other documentation for system authorization, are available at the IRM/IA Web site, setup to help system owners achieve system authorization.

5 FAH-11 H-212.3-1 Documentation Review

(CT:IM-4; 06-13-2007)

a. The certification analyst must review the documentation of a system undergoing certification to verify that the minimum required baseline controls are implemented for the system/application, and that the confidentiality, integrity and availability of information is protected commensurate with the classification and sensitivity level of information processed.

b. If the documentation does not accurately describe the system/application and/or required controls, or if it is determined that the documentation is incomplete or inaccurate, the certification analyst must:

(1) Generate a Document Change Request (DCR) that will detail documentation deficiencies and provide recommendations to correct the deficiencies; and

(2) Return the documentation to the system owner for correction and/or update. In this case, the certification analyst must specify to the system owner in writing what information in the documentation is not in accordance with Department standards.

c. After the certification analyst considers the required documentation as adequate, the certification analyst will record the documentation as part of the system's C&A, and the process progresses to Certification (Phase II).

d. The system manager must review the system's completed documentation for compliance with Department standards at least annually, or when a system's authorized baseline configuration undergoes a significant change, or as directed to meet re-certification requirements.

5 FAH-11 H-212.3-2 Security Control Assessment

(CT:IM-4; 06-13-2007)

a. After the initial technical document review is completed, the certification analyst must provide the system owner with an approved Security Control Assessment Plan (SCAP). Details in the SCAP must include:

(1) The requirements for network access and the types of automated tools, checklists, and other functions that will be used when accessing the network.

NOTE: Generally, in follow-up, the certification analyst may explain via e-mail to the system owner the type of network access needed to perform certification assessment);

(2) The details required for authorized access to the workspace that the certification analyst is authorized to access. As applicable, each certification analyst will need to obtain a domain administrator, application administrator, and application user account; and

(3) A requirement to review the Systems Categorization, SSP, CP, Privacy Impact Assessment (PIA), Security Impact Statement and other key documentation provided by the system owner;

(4) Workspace requirements for the systems authorization team members performing the system's certification; and

(5) Approval requirements allowing the certification team members ongoing access to the test site and/or equipment (if required).

NOTE: To prevent possible schedule delays in certification of the system, it is essential that ongoing access requirements be coordinated with and approved by the system owner, system manager, and/or local ISSO well in advance of initiating system certification.

b. If the system owner requires it, the certification analyst schedules a meeting to review the SCAP with the system manager and local ISSO. The SCAP may include documentation showing CISO approval to perform "Social Engineering" if the system contains highly sensitive information (e.g., HIPAA or Privacy Act information), or is classified up to Secret. Social engineering is defined in NIST IR 7298.

c. The certification analyst must be prepared to answer technical questions about the proposed testing as posed from the customer.

5 FAH-11 H-212.3-3 Phase I Completion

(CT:IM-4; 06-13-2007)

a. To complete Phase I requirements of the System Authorization Process and move to certification (Phase II), system owners must ensure the following:

(1) Required documentation is completed to Department standards. Documentation must include, but is not limited to:

(a) Security Categorization Form, also referred to as IT Asset Categorization form;

(b) Automated and manual configuration scan results;

(c) System Security Plan (SSP);

(d) System Contingency Plan (CP), where required;

(e) Privacy Impact Assessment;

(f) Common software weakness listing of commonly known vulnerabilities (if any). The standard for information security vulnerability names is found in the Common Weakness Enumeration (CWE) list;

(g) Report results from general audits and infrastructure vulnerability assessments dealing with system certification:

- General Accounting Office (GAO) audits;
- Financial system audits;
- Critical infrastructure vulnerability assessments; and
- Independent Auditor audits.

(h) System technical diagrams (less Internet protocol (IP) addresses) of current system configuration and baseline of operation;

(i) E-authentication assessment, reference OMB M-04-04;

NOTE: If a system is subject to E-authentication, the system must be reported in the annual report to OMB;

(j) Information Technology Applications Baseline (ITAB) registration of software and hardware for identified systems having unregistered software installed as part of the system's operational baseline;

(k) Current self-assessment, where required. (See NIST SP 800-26, Revision 1, Appendix A.); and

(l) Approved IT CCB System Authorization Request (see IT CCB SOP);

(2) If other relevant documents are available, the certification analyst may request them from the system owner via e-mail, with courtesy copy [cc:] to IRM/IA; and

(3) The certification analyst must review the Bureau-provided documentation, regarding system information, to gain an understanding of the target application and its platform. Other documentation relevant to certification may include, but not be limited to:

(a) Systems manual;

(b) Standard operating procedures;

(c) Network topology;

(d) Data flow diagram; and

(e) Application user and/or security manuals.

b. The Systems Authorization Process may not progress from Initiation (Phase I), to Certification (Phase II) until the following tasks are accomplished:

(1) Assignment of the systems authorization team;

(2) Establishment of the system's C&A work plan (with milestones and resource requirements); and

(3) Completion of all required documentation to Department standards.

5 FAH-11 H-212.4 Certification Phase

(CT:IM-4; 06-13-2007)

Certification is Phase II of the Systems Authorization Process (see 5 FAH-11

H-300, System Authorization).

5 FAH-11 H-212.4-1 Certification Baseline

(CT:IM-4; 06-13-2007)

a. When performing system certification, the certification analyst must use the security documentation assembled and recorded by the bureau as the baseline for formal assessment of the system's accreditation boundary and validation of the system's security controls.

b. All documentation assembled for certification of a system must include the security documentation that the Department requires to complete the Systems Authorization Process.

c. The system's accreditation boundary and minimum required security control baseline, as determined using the security categorization impact level, must be established in the system's security documentation before certification can begin.

5 FAH-11 H-212.4-2 Certification Milestones

(CT:IM-4; 06-13-2007)

a. Certification milestones must include completion of pre-certification, certification, and post-certification.

b. During pre-certification, a certification analyst must:

(1) Gain an understanding of the system's operations and identify the computer-related operations significant to preparing the SCAP (previously referred to as security test & evaluation (ST&E));

(2) Ensure the system owner has approved the security categorization level and subsequent rigor of the SCA;

(3) Identify the management, operational and technical security controls that will be tested in the SCA; and

(4) Use the appropriate low, moderate, or high impact certification checklist and make a preliminary assessment on whether management, operational, and technical security controls are likely to be effective:

(a) The certification analyst's evaluation of computer-related controls is critical and must be planned in conjunction with other aspects of the system's operating environment, (e.g., developing and significant computer-related activities at multiple locations that may affect a connecting system's operation or its security posture);

(b) The certification analyst must submit the proposed SCAP to the designated Lead Certifier for approval; and

(c) A detailed description of SCA activities and specific dates for testing must be established and communicated to the system owner.

(5) Upon approval of the proposed SCAP, notify the system owner of the pre-certification tasks that will be performed in the SCAP.

c. During Certification (Phase II), a certification analyst must:

(1) Conduct a site survey; the goal of which is to:

(a) Verify the accuracy and completeness of the system's documentation;

(b) Collect preliminary information that will supplement the SCAP; and

(c) Verify the status of the system to be tested, whether a stable baseline exists, and whether or not the:

(i) SSP accurately represents the system's current configuration and accreditation boundary;

(ii) System's baseline configuration is stable and correctly represented in the SSP; and

(iii) CP, if required, accurately reflects its operating environment and system requirements to return to full operation in the event that risk is realized.

(2) Perform a comprehensive technical evaluation to verify if the system is compliant with Department security configuration documents and standards:

(a) The certification analyst must follow the C&A work plan, which must be based on the initial review of pre-certification documents submitted by the system owner and results of the site survey;

(b) Example topics and draft questions a certification analyst may address in the technical evaluation and SSP review are:

(i) The scope of the SCA. Determined by asking - Which machines support the system? Who are the parties involved in the system operations? What is the location of the support facilities?

(ii) The impact level of a security control may be assessed by asking the system owner questions that help to determine the impact if a threat exploits a vulnerability and results in loss of system confidentiality, integrity or availability. Determined by asking - How long can the system be down before it affects the Department or Bureau’s mission? What would happen to the Department’s mission if system availability is affected for a period greater than one, two, three hours, etc.

(iii) The accreditation boundary may be determined by asking questions that establish systems and/or applications limitations included in Certification. Determined by asking - Where does the application or system processing boundary stop? What are the logical and physical interfaces where data is passed to/from another system?

(iv) The resources. In determining the resources that may be required to support a SCA, the certification analyst may ask directly - What are your available resources to support requirements with respect to certification efforts?

(v) The timeline. A tentative timeline could be established by asking – What is the system target authorization date? How long will it take to certify the system?

(3) Plan, conduct, and report SCA results.

(a) The SCAP must be:

(i) Based on documented security requirements within the accreditation boundary, and the security categorization impact level determined for the system; and

(ii) Developed from detailed checklists and configuration guides that match the system or network characteristics (i.e., network topology diagrams and system data flow processes).

(b) The SCA results must list remediation items required by FAM or FAH that must be remediated according to the Plan of Action and Milestones (POA&M), also referred to as the corrective action plan.

(4) Communicate to the system that all remediation actions must be recorded and tracked to completion, using the Department’s automated POA&M tool (see the Department’s Performance Measures and POA&M Process Guide on the Information Assurance Web site); and

(5) Work with the system owner to clarify any issues with significant vulnerabilities caused by poorly implemented or missing controls that may require prioritizing for immediate remediation.

d. During post-certification, the certification analyst:

(1) Compiles testing results and develops the Certification Package (e.g., Phase II), which includes the Certification Report identifying compliance weaknesses and recommended system remediation; and

(2) Ensures the Certification Report contains:

(a) Deficiencies noted in the system's management, operational and technical security controls, including insufficient or missing documentation (e.g., SSP, CP);

(b) All positive findings contrary to Department security configuration standards posted on the DS/SI/CS Web site,;

(c) Any active external findings that apply to the system under evaluation from the Office of Inspector General (OIG), the Independent Auditor, or the Government Accountability Office (GAO);

(d) The identified common vulnerabilities and exposures (CVE) listed in NIST's National Vulnerabilities Database; and

(e) Recommendations for remediation as a best security practice. See the NIST Web site for Federal Government best practices.

NOTE: Optional recommendations for remediation of risk are not required by FAM or FAH, but must be remediated as a best security practice).

5 FAH-11 H-212.4-3 Certification Tools, Software, and Equipment

(CT:IM-4; 06-13-2007)

a. In the system's established C&A work plan, the certification analyst, if a Federal employee, must use a laptop configured with Department-approved software/hardware and certification tools.

b. A contract non-government certifier must coordinate with the system owner to ensure that a Department-owned laptop, configured with Department approved software/hardware and certification tools, is used.

NOTE: To avoid delays in certification, the certification analyst must ensure the software and equipment necessary to conduct the SCA are acquired as soon as feasible.

5 FAH-11 H-212.4-4 SCAP Development Requirements

(CT:IM-4; 06-13-2007)

a. The certification analyst must demonstrate to the system owner that the security control assessment plan (SCAP):

   (1) Outlines the certification analyst's plan to assess and validate a system's required minimum baseline security controls;

   (2) Specifies the management, operational and technical security controls that will be tested;

   (3) Is developed and based on the security impact level, which drives the test procedures;

   (4) Uses the appropriate certification checklist; and

   (5) Is developed and coordinated with the system manager.

b. The system manager coordinates the development, scope, and complexity of the SCA.

c. The system owner approves the SCAP.

d. The system owner or sponsoring bureau must ensure the test procedures are formally approved and documented in the SCAP before certification can begin.

5 FAH-11 H-212.4-5 Executing The SCAP

(CT:IM-4; 06-13-2007)

a. Executing the SCAP includes testing and validating the security controls implemented for operating software, enterprise applications and hardware configurations that may comprise the system undergoing certification.

b. The certification analyst must inspect a system's in-place security controls using the appropriate certification checklist, which requires thorough review of:

   (1) Operational controls, including but not limited to:

      (a) Personnel security;

      (b) Physical security;

      (c) Production, input/output controls;

      (d) Contingency planning (where required);

      (e) Hardware and systems software maintenance procedures;

      (f) Data integrity;

      (g) Documentation;

      (h) Security awareness, training, and education; and

      (i) Cyber-security response capability.

(2) Management controls, including but not limited to:

(a) Risk management;

(b) Review of security controls established within the accreditation boundary;

(c) Life cycle monitoring;

(d) Authorize processing (C&A); and

(e) SSP and the CP.

(3) Technical controls, including but not limited to:

(a) Identification and authentication (to system);

(b) Logical access controls (to the enterprise applications); and

(c) Audit trails (i.e., related to physical access, system authentication, and application access).

c. A certification analyst must use only Department-approved software/ hardware tools to identify all possible weaknesses and vulnerabilities that may exist in a system.

NOTE: Any additional tools that may be required for certification of a system, which are not on the approved list, may only be used after submitting a change request and attaining IT CCB approval.

5 FAH-11 H-212.4-6 Analyzing Server Software Controls

(CT:IM-4; 06-13-2007)

a. A system’s server must be configured with the core baseline applications approved by the IT CCB, or where appropriate the local CCB. See Department configuration requirements posted on the IT CCB Web site.

b. When analyzing the server software controls (e.g., operating system):

(1) A certification analyst must check against Department server security configuration standards, posted on the DS/SI/CS Web site;

(2) Deviations from the Department approved security configuration standards must be documented in the SSP; and

(3) Any discrepancies or differences with Department server security configuration standards must be assessed for validity, and if invalid, documented in the findings table:

(a) False-positive findings are those findings that indicate a system is mis-configured to Department standards, but may be configured according to local CCB-approved configuration requirements, or as an existing exception to policy; and

(b) Positive findings are identified and catalogued in the

Certification Report, which is generated as part of Phase II requirements.

c. The server's operating system service pack level and installed hot fixes must also be checked.

d. Detailed information on IT CCB approval process to add to or subtract from a system's approved baseline configuration is available on the Department's IT CCB Web site.

5 FAH-11 H-212.4-7 Evaluating Workstation Software Controls

(CT:IM-4; 06-13-2007)

a. A system's workstation must be configured with the core baseline applications approved by the IT CCB. For more information on this process, see the IT CCB Web site.

b. When evaluating a workstation's operating system:

(1) A certification analyst must check against Department security configuration standards for the workstation's current, installed operating system. For more information on this process, see the DS/SI/CS Web site;

(2) Deviations from Department-approved security configuration standards must be documented in the SSP; and

(3) Any discrepancies or differences with Department workstation security configuration standards, documented in the SSP, must be assessed for validity, and if invalid, documented in the findings table as follows:

(a) False-positive findings are those findings that indicate a system is mis-configured to Department standards, but may be configured in accordance with local configuration requirements, or as existing exception to policy allows; and

(b) Positive findings are identified and catalogued in the Certification Report generated as part of Phase II requirements.

c. The service pack level for Windows-based workstation's operating system and installed hot fixes must be checked.

NOTE: This is accomplished by using the Department's automated configuration tool to check the configuration of the workstation's operating system against Department security configuration standards.

5 FAH-11 H-212.4-8 Enterprise Applications

(CT:IM-4; 06-13-2007)

a. The SCAP must include all enterprise application software designed and installed to support Department mission requirements.

b. A system's enterprise application software may consist of major applications configured or modified to support specific user needs. Therefore, enterprise software may consist of any combination of the following:

(1) Commercial-off-the-shelf (COTS);

(2) Government-off-the-shelf (GOTS); or

(3) Software programs developed in-house to specifically support the mission of the bureau, office, or division, or to satisfy a specific set of user requirements.

c. An enterprise application is defined as major if any of the following applies:

(1) Typical purpose is to support a specific mission-related function and the required security controls are not covered by the GSS;

(2) Requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application;

(3) Must be certified as a major application under the Systems Authorization Process;

(4) Is classed as Critical Infrastructure;

(5) Processes National Security Information (NSI); or

(6) Has significant impact on performance of a general support system (GSS).

d. Unless otherwise approved by the local CCB, a system's enterprise software may only consist of the core baseline applications approved by the IT CCB (see the IT CCB Web site).

e. The system's enterprise software must be analyzed and checked in the same manner as listed in above paragraph H-212.4-5.2 as referenced for a system's operating system.

f. The operating system (OS) of the server hosting the enterprise application for the respective software package must also be checked against the Department's security configuration checklist (e.g., if the server that supports the enterprise application is configured with Windows 2000 Server, then the checklist for Windows 2000 Server must be used during system certification).

g. A certification analyst must review specialized documents that are generated for the use of the enterprise application, (e.g., user manuals and documentation).

5 FAH-11 H-212.4-9 Identifying Operational Requirements

(CT:IM-4; 06-13-2007)

a. To identify and understand an application's operating parameters, the certification analyst must set up a demonstration of the application with a subject matter expert (SME) who regularly uses the application, or who may have developed or helped develop the application.

b. The certification analyst must discuss a system's operational requirements with other key personnel, including but not limited to:

   (1) System owner and system manager: To obtain general information on procedures, functions, and visibility of the enterprise application;

   (2) Local ISSO: To assess information on security procedures (logon, passwords, security policies, audit procedures/review and contingency plans);

   (3) System administrator, developer, or database administrator (DBA): To obtain information on technical issues, technical policies, and the administrative procedures of the enterprise application; and

   (4) Users who regularly use the enterprise application have accumulated knowledge on the general functionality, usability, and problems encountered when using the enterprise application in day-to-day operations. Users may be helpful in pointing out security flaws, operational concerns, and any management issues the enterprise application may have.

c. Whenever possible, the certification analyst should test the functionality of the enterprise application to ensure it is functioning as designed and required.

d. In the course of testing the enterprise application, the certification analyst must document all vulnerabilities and issues that may be considered weaknesses.

   (1) If the enterprise application has a database back-end (Primarily, Structured Query Language (SQL) or Oracle Software), then the lead certification analyst must ensure the team includes the appropriate expertise in these areas;

   (2) In preparation of testing the database, a certification analyst certifying the database must:

      (a) Contact the bureau's database administrator (DBA) to schedule a time to conduct the database review for the application;

(b) Compare Department checklists to the database installation;

(c) Run appropriate scripts for the installed database to review the logical access control structure (**NOTE**: It is important to match testing scripts to run with the version of database installed); and

(d) Review the list of users and administrators that access the database as well as their permissions or roles performed in accessing the database.

(3) Findings, identified during the database review, must be transferred from the database checklist document to a final database findings table report document. Each finding must be given a potential impact rating of low, moderate or high (see FIPS 199);

(4) Upon completion of the database findings table for the application, and in accordance with Department internal review processes, the certification analyst must forward this material to the lead certification analyst for incorporation into the Certification Report as part of Phase II requirements; and

(5) The certification analyst must coordinate the analysis of the business impact assessment of each technical finding identified and recorded in the Certification Report with Risk Management.

e. A certification analyst must:

(1) Perform checks on the assigned user roles for each application that interfaces with the system (e.g., Admin, User, DBA, etc.);

(2) Verify that data input to the application maintains its integrity. The process testing for this step must include procedures to:

(a) Check whether or not the application data directory's NTFS permissions are set correctly—not to exceed the maximum number of authorized users allowed to access the application;

(b) Evaluate the application's reporting and audit capabilities (e.g., the certifier must verify the application's auditing is enabled within the parameters prescribed by its configuration standard); and

(c) Review the application audit logs.

(3) Verify that the application data output maintains its integrity. Process testing for this step must:

(a) Verify that an existing backup for the application is in place and the backup facilities meet requirements outlined in the CP; and

(b) Employ a system audit that determines where the application backups are stored and whether storage facilities are used in conjunction with a Contingency Plan (CP).

5 FAH-11 H-212.4-10 Output Testing

(CT:IM-4; 06-13-2007)

a. For audit purposes, the certification analyst must obtain from the system owner current copies of all Change Control Board (CCB) approvals of installed enterprise software applications (COTS/GOTS), whether approved by local CCB, or IT CCB. The certification analyst must also obtain copies of approved deviations from Department configuration standards. During certification, all installed applications that are identified as not on the local CCB-approved or IT CCB-approved list, must be reported and subsequently submitted to the appropriate CCB for approval.

b. The security level necessary to protect a system's physical environment must also be verified. Therefore, the certification analyst assigned to certify the system must evaluate the location-specific common controls to verify that the physical facility hosting the application's supporting server(s) is secured in accordance with Department requirements.

c. For enterprise applications, a certification analyst must evaluate existing:

(1) Security systems;

(2) Fire protection systems;

(3) Operating environment and general integrity of the system (e.g., Classified information displayed on a monitor is not viewable from outside facing windows); and

(4) Security memos, authorizations or certifications the facility received.

d. A certification analyst must evaluate installed hardware installations, using the configuration baselines established and approved by the IT CCB and/or the local CCB, including:

(1) Workstations and laptops;

(2) Supporting servers;

(3) Switches, biometrics, etc.; and

(4) IT equipment used to host or access the application.

5 FAH-11 H-212.4-11 Analysis and Reporting

(CT:IM-4; 06-13-2007)

a. After performing the SCA test, a certification analyst must:

(1) Review the data and verify the security vulnerability findings;

(2) Create a list of the findings and forward it to the system owner;

(3) Discuss the vulnerability findings with the system owner to identify any mitigating controls;

(4) When requested by the system owner, and if resource allocations allow, assist the system manager to perform the mitigation measures they are able to perform within the specified period, designated in the C&A work plan; and

(5) Update the findings.

b. SCA results and analysis must be compiled into a Certification Report and forwarded to Risk Management for validation and evaluation of business impact and risk.

5 FAH-11 H-212.4-12 Review Process

(CT:IM-4; 06-13-2007)

a. The lead certification analyst reviews the Certification Report to ensure that a system's boundary is accurately assessed. The review must cover two areas:

(1) All scan results, including penetration test results if conducted; and,

(2) The findings table that tabulates scan results from database assessments, interviews, and checklists used in the SCAP.

b. If a business need exists, the system owner must justify implementation of the system in the production environment prior to remediation of a finding:

(1) The certification analyst must validate that the business need justifies the request, and appropriately addresses the deficiency cataloged by the (non-remediated) finding;

(2) The lead certification analyst must include all requests, submitted by the system owner for approval, in the Certification Report; and

(3) The risk analyst must evaluate each request included in the Certification Report for its business impact and level of risk (high, medium, or low) to Department systems.

c. Once the lead certification analyst completes the review and there are no issues, the Certification Report is finalized and the process may continue to Phase III of the Systems Authorization Process.

d. The system owner must ensure that key systems authorization team members are notified of the status of the application or GSS.

5 FAH-11 H-212.4-13 Review Meeting

(CT:IM-4;   06-13-2007)

a. The review meeting (previously referred to as the findings meeting) is convened at system owner's request and must be composed of key stakeholders having an interest in C&A of the system.

b. If requested, the risk manager will initiate the review meeting to review all findings and associated POA&M.

c. The schedule for remediation of a system's identified vulnerabilities must be recorded in POA&M format for ease of reporting.

5 FAH-11 H-212.4-14 Risk Mitigation

(CT:IM-4;   06-13-2007)

a. Medium and high risk must be remediated, unless:

   (1) A business need overrides the security concerns and all efforts and resources to reduce risk to low are exhausted; and

   (2) The DAA accepts the (medium and high) risk by authorizing the system to operate until the remediation is implemented.

b. Risk mitigation options are discussed in detail in NIST SP 800-30, Risk Management Guide for Information Technology Systems.

5 FAH-11 H-212.4-15 Verification And Validation

(CT:IM-4;   06-13-2007)

a. When the system owner mitigates a finding, the certification analyst, and where appropriate the database administrator (DBA), must verify and validate that remediation of a finding meets Department requirements to lower risk to an acceptable level (low).

b. Once remediation of a finding is validated, the certification analyst updates the Certification Report and submits it to Risk Management for review and confirmation of risk.

c. The Certification Report submitted to Risk Management for validation must reflect all updates and corrections, as verified and validated by the certification analyst and/or DBA.

5 FAH-11 H-212.4-16 End of Phase Requirements

(CT:IM-4;   06-13-2007)

Once the certification analyst completes the Certification Package to Department standards, Certification ends and the process may move to the next phase (Phase III -Authorization).

5 FAH-11 H-213 THROUGH 219 UNASSIGNED