

5 FAH-11 H-400 SYSTEM AUTHORIZATION OF NON- DEPARTMENT SYSTEMS

5 FAH-11 H-410 GENERAL

(CT:IAH-5; 06-25-2007)
(Office of Origin: IRM/IA)

5 FAH-11 H-411 INTRODUCTION

5 FAH-11 H-411.1 Purpose

(CT:IAH-5; 06-25-2007)

- a. This subchapter establishes procedures to implement system authorization of non-Department entity systems that process information on behalf of the Department as set forth in 5 FAM 1065.1-6. These systems either connect to Department information systems, or process/store Department information without establishing a connection.

NOTE: Non-Department entity refers to U.S. Government civilian and military personnel, consultants, contractors, foreign, state, local governments or organizations, and other individuals that require access to Department information systems. This includes entities that provide Information Technology (IT) services and related computer industry support that contribute to the efficient functioning of the Department.

- b. This subchapter will assist sponsoring bureaus to implement processes that protect Department information and information systems from operational, strategic, and legal risks that a non-Departmental system may present.
- c. The Non-Department System Authorization Process is designed to certify that a non-Departmental system meets documented security requirements, and will continue to maintain the accredited security posture throughout the authorized system's life cycle.

5 FAH-11 H-411.2 Objective

(CT:IAH-5; 06-25-2007)

- a. The Federal Information Security Management Act of 2002 (FISMA) requires that all systems that process or store Department information must be certified and accredited.
- b. Implementation of this subchapter will help to enable secure information exchange, collaboration, and interoperability among Department bureaus and other federal, state, and local agencies.
- c. The Office of Information Assurance (IRM/IA) is the responsible office for the contents of this chapter. Send questions or comments to the IRM/IA e-mail address, informationassurance@state.gov.

5 FAH-11 H-411.3 Scope

(CT:IAH-5; 06-25-2007)

- a. This subchapter outlines the procedures that must be met to achieve non-Department system authorization. Types of connectivity to Department information systems are identified in 5 FAH-11 H-800, Connections to Non-Department Entities.
- b. Bureaus that sponsor non-Department system authorization must use the process established in this subchapter to meet the Designated Approval Authority's (DAA) authorization requirements whether or not connectivity is achieved.
- c. These procedures exclude authorization of Sensitive Compartmented Information (SCI) systems. Systems that process or store national security level information are processed for authorization in accordance with applicable Federal and Department requirements for authorization of classified and SCI systems (see 12 FAM 630, 12 FAH-6, and NISPOM-Chapter 8, DD-254, and DOSAR). The Bureau of Diplomatic Security (DS) is the DAA for SCI systems at the Department (see 1 FAM 271.1 d).
- d. This subchapter does not apply to non-Department systems used with the Department's telework solution. (See 12 FAM 091 for definition of automated information system.)

5 FAH-11 H-411.4 Oversight Of Non-Department System

(CT:IAH-5; 06-25-2007)

- a. The Department, as required by FISMA, must ensure that non-Department entities develop, implement, and maintain a baseline of minimum security controls to protect Department information and information systems. The policy requirements for non-Department systems are set forth in 5 FAM 1065.1-6.
- b. In 2005, the Department developed, documented in its Information Security Program Plan (ISPP) (under Management Plan), and implemented an ongoing Department-wide information security program to protect its information and information systems. This program details the oversight management which extends to those non-Department systems delivering IT systems and services to or on behalf of the Department.

5 FAH-11 H-411.5 Key Personnel

(CT:IAH-5; 06-25-2007)

- a. Key personnel, identified to perform certification and accreditation (C&A) of a non-Department system, must not be involved with its development, implementation, or operation (see 5 FAM 1065.1-4), or be under the sponsoring bureau's direct management authority.
- b. Members of the authorization team must consist of a combination of key staff members assigned to participate in C&A of a system when operating under Department authority. Authorization team members must have the appropriate level of experience and credentials for the positions assigned. They must also be able to fulfill the responsibilities of the following roles:
 - (1) Sponsoring Bureau Representative;
 - (2) System manager and/or vendor representative;
 - (3) Certification team lead (must be independent for moderate or high impact systems);
 - (4) Certification analyst(s) for operating system and database;
 - (5) Risk Management team lead;
 - (6) Risk analyst;
 - (7) User representative (where needed); and
 - (8) Other key participants having an interest in the C&A outcome.

- a. Non-Department entities must furnish their results for any non-Department system independent C&A to the Sponsoring Bureau Representative and to IRM/IA for compliance evaluation with the requirements of this subchapter.
- b. Key staff members working to certify and accredit a system must:
 - (1) Coordinate user participation, when necessary;
 - (2) Participate in reviews and interviews; and
 - (3) Provide review and input for the team’s deliverables.
- c. Authorization team members may perform multiple roles or several members may work together to fulfill one role since duties may vary based on the nature of the accreditation task.

5 FAH-11 H-412 ROLES AND RESPONSIBILITIES FOR NON-DEPARTMENT SYSTEMS AUTHORIZATION

5 FAH-11 H-412.1 Designated Approval Authority (DAA)

(CT:IAH-5; 06-25-2007)

- a. The Chief Information Officer (CIO) is the Designated Approval Authority (DAA) for systems at the Department that are designated unclassified up through collateral Top Secret (TS). The DAA approval requirements must be stated in the formal agreement established by contractual arrangement between the sponsoring bureau and the non-Department entity. The CIO makes the decision to authorize or deny authorization of a non-Department system. (See 1 FAM 271.1 d.)
- b. The Bureau of Diplomatic Security (DS) is the DAA for State systems that fall under the requirements of the Director of Central Intelligence (DCI) Directive for Protecting Sensitive Compartmented Information (SCI) Within Information Systems.
- c. The CIO also works with program officials, budget officers, Inspectors General, and other appropriate agency officials, to develop a Plan of Actions and Milestones (POA&M) report to the Office of Management and Budget (OMB) for each non-Department system for which a weakness is identified during annual FISMA reports. The IRM/IA Web site contains

requirements and instructions for completing the POA&M.

5 FAH-11 H-412.2 Chief Information Security Officer (CISO)

(CT:IAH-5; 06-25-2007)

- a. The Chief Information Security Officer (CISO) heads IRM/IA and oversees and manages compliance with the requirements imposed on the sponsoring bureau during authorization of a non-Department system under the CIO's direction. (See 44 U.S.C. 3544.)
- b. The CISO defines and oversees the process and requirements for meeting a non-Department system authorization.

NOTE: The independent certification authority performing certification of a system must show that the level of information security is appropriate to protect the integrity, confidentiality, and availability of Department information and information systems.

5 FAH-11 H-412.3 IRM/IA

(CT:IAH-5; 06-25-2007)

IRM/IA evaluates a percentage of the completed system authorization packages to ensure compliance with Department C&A processes and standards.

NOTE: Requirements for independent certification are in 5 FAM 1065.1-4.

5 FAH-11 H-412.4 Sponsoring Bureau

(CT:IAH-5; 06-25-2007)

- a. The bureau sponsoring authorization of a system is responsible for the secure operation of Department information systems accessed by a non-Department system. The sponsoring bureau must ensure that controls are in place to protect Department information that is processed or stored at a non-Department entity's facility.
- b. The sponsoring bureau must ensure that the supporting documentation required for DAA authorization of a non-Department system is generated.

NOTE: Refer to the documentation requirements in 5 FAH-11 H-820 for establishing and governing connections with non-Department entities in

instances where connectivity is an issue.

- c. The sponsoring bureau must send a memo to the CISO explaining the basic functions and purpose of the system and indicating that the system is entering into the Non-Department System Authorization Process. Once a system is entered into the Non-Department System Authorization Process, the sponsoring bureau must:
- (1) Exercise program control over Department information systems under their management authority that will exchange information with a non-Department entity that is allowed access to process or store information on behalf of the Department;
 - (2) Represent the non-Department system's interest to the Department throughout its lifecycle;
 - (3) Ensure that the non-Department entity establishes and documents the unclassified and classified baseline security control configuration for the information system seeking DAA authorization (see Department of State Security Control Baseline Process and Security Control Catalog For Unclassified Systems, and 12 FAM 630). The identified security controls must be documented in the system's System Security Plan (SSP) and Contingency Plan (CP) as generated by the non-Department entity;
 - (4) Register the system in the Information Technology Application Baseline (ITAB), and ensure the system's security categorization process is completed in the ITAB in accordance with Department requirements. (See the ITAB Web site) for more information);
 - (5) Ensure that the non-Department entity completes the security categorization for unclassified systems in accordance with the latest FIPS Publication 199 requirements;
 - (6) Determine the sensitivity level of Department information processed or stored in the system, and define the functions users are permitted to perform when accessing the system;
 - (7) Ensure that the non-Department entity implements system baseline security controls that meet federal mandates to protect information commensurate with its sensitivity level and classification and assure the controls are in compliance with Department policy and guidelines for security control selection:
 - (a) **Unclassified Systems:** The categorization of information must determine the impact level (see FIPS Publication 199 and NIST Special Publication (SP) 800-60) of the processing

system, and, as categorized, minimum baseline controls must be implemented in accordance with the Security Control Baseline Process and Security Control Catalog for Unclassified Systems; and

- (b) **Classified Systems:** The classification of the information (Confidential, Secret, Top Secret), combined with availability and integrity impact, must
 - (i) Determine the baseline controls from the National Industrial Security Program Operating Manual (NISPO) Chapter 8, DD-254, Department of State Acquisition Regulations (DOSAR), and Department specific controls identified for systems processing or storing classified information on behalf of the Department; and
 - (ii) Supplement the security control baseline in accordance with Department policy (see 12 FAM 630 and 12 FAH-6);
 - (8) Identify key stakeholders that will participate as members of the independent accreditation team. This includes identifying the user representative for the system, and sponsoring bureau participants appointed as facilitators to handle key functions that support C&A of the system;
 - (9) Identify, assess, prioritize, and monitor the progress of corrective efforts (remediation) of security weaknesses (vulnerabilities) found in the system under the sponsoring bureau's management authority; and
 - (10) Work with the CIO to report to OMB the status of implementation of planned security controls and/or remediation of identified deficiencies of the system security controls listed in the system's POA&M report. The quarterly submissions of POA&M reports to OMB should include, but not necessarily replace, all Department security remediation plans. (See OMB memorandum M-01-24 for guidance on reporting the results of security reviews and evaluations.)
- d. Systems currently processing or storing information on behalf of the Department without authorization from the DAA must be immediately reported to DS/SI/CS and IRM/IA. Also report systems connected to the Department's networks to IRM/OPS. All non-Department systems must be entered into the Non-Department System Authorization Process by the sponsoring bureau. The sponsoring bureau must notify DS, IRM/OPS and IRM/IA with the required system information. The CIO may deny

authorization of the system if the sponsoring bureau fails to enter the unauthorized system into the Non-Department System Authorization Process.

- e. The sponsoring bureau must coordinate and monitor the activities of information security practitioners assigned to independently certify and accredit a non-Department system.

NOTE: Independent certification is required for moderate or high impact level unclassified and all classified systems. Low impact systems do not require independent certification.

5 FAH-11 H-412.5 Certification Team

(CT:IAH-5; 06-25-2007)

- a. The certification team must ensure all required controls specified in the SSP of a non-Department system that processes or stores Department information have been appropriately scoped and are addressed.
- b. The certification team must evaluate all controls specified in the non-Department system SSP to the level of rigor required for the system's designated impact level.
- c. Only the Lead Certifier must meet the requirements for independence as specified in 5 FAM 1065.1-4 in circumstances where independent certification is required.
- d. All certification analysts must perform certification in accordance with 5 FAH-11 H-200, Certification (Information Security Audit).

5 FAH-11 H-412.6 Authorization Team

(CT:IAH-5; 06-25-2007)

- a. The authorization team is responsible for scoping the initial security control baseline by using an assessment of risk and potential harm to the Department's mission from a non-Department system and documenting the resulting baseline in the SSP.
- b. The authorization team analyst assigned to assess risk for a system undergoing accreditation under the Non-Department System Authorization Process must perform the following activities:
 - (1) Assess and document the risk and potential impact posed from this system which accesses Department information and information

systems;

- (2) Evaluate, determine the scope, and identify the minimum security controls to meet the requirements in this subchapter for unclassified systems. The analyst must use the results of the documented risk and potential impact posed from this system. (See the latest Security Control Baseline Process and Security Control Catalog for Unclassified Systems process guide, available on the IRM/IA Web site);
 - (3) Ensure that all requirements mandated in 12 FAM 600, 12 FAH-6, Chapter 8 of the National Industrial Security Program Operation Manual (NISPOM), and the DD-254 Contract Security Classification Specification have been incorporated into the SSP for classified non-SCI systems; and
 - (4) Recommend the level of managed risk to the DAA for authorization approval or denial upon completion of the system certification.
 - (a) Systems with overall high residual risk require the authorization team analyst to make a recommendation to the DAA to deny authorization. Systems with overall medium residual risk require the authorization team's analyst to make a risk-managed authorization recommendation to the DAA based upon information supplied by the sponsoring bureau. This may include, but is not limited to, business need, scoping justifications, compensating security controls, and reasonable completion dates for remediation of medium risk items. The recommendation to the DAA may be to
 - Grant the system a full authorization for 36 months,
 - Grant a full authorization for less than 36 months,
 - Grant a full authorization with stipulations pertaining to remediation of medium risk items, or
 - Deny authorization; and
 - (b) Systems with low risk require the authorization team analyst to make a recommendation that the DAA approve authorization.
- c. Besides a recommendation to the DAA to approve or deny a non-Department system authorization, the Authorization Memorandum generated by the authorization team analyst must include:

- (1) A brief description of the system operating environment and accreditation boundary, including hardware/software configurations, and the applications that fall within the accreditation boundary;
- (2) A detailed presentation of the assessed risk affecting the authorization decision; and
- (3) The system's initial POA&M report.

NOTE: This report must translate the results of the Certification Report into the standard POA&M format, and should be used to facilitate communication back to the sponsoring bureau concerning the vulnerabilities found in connecting to a system.) (See the IRM/IA Web site for more information on preparation and use of the Authorization Memorandum.

5 FAH-11 H-413 PROCEDURES FOR SYSTEM AUTHORIZATION OF NON-DEPARTMENT SYSTEMS

5 FAH-11 H-413.1 General

(CT:IAH-5; 06-25-2007)

- a. Non-Department entities must undergo system authorization under the Non-Department System Authorization Process if:
 - (1) The sponsoring bureau demonstrates a business need that the non-Department entity fills; or
 - (2) Department information is being, or is planned to be processed or stored on a non-Department system; or
 - (3) Department required legal contractual arrangements are in place between the sponsoring bureau and the non-Department entity.
- b. The sponsoring bureau facilitates certification and accreditation (C&A) of a non-Department system. The four aspects that encompass C&A are:
 - (1) **Technical review and evaluation:** Verify through independent technical review and evaluation the existence of the minimum required security controls in and around the system for low, moderate, and high impact unclassified and all classified systems;

- (2) **Testing:** Test the effectiveness of the implemented or planned baseline security controls. These controls must provide sufficient protection, commensurate with the level of information that the controls protect;
- (3) **Risk-managed processes:** Involve senior management in the security lifecycle, and provide sound operational decisions, based on an identified, objective, risk-managed process; and
- (4) **Authorization:** Achieve full authorization to operate for the maximum time allowable, up to three years, using a risk-management process. Authorization requires that:
 - (a) Mission effectiveness is balanced with security requirements and risk management;
 - (b) Appropriate officials are assigned to manage responsibilities commensurate with their designated roles and security responsibilities; and
 - (c) Authorization of systems that process or store Department information is achieved either prior to operations, or as currently operational.

5 FAH-11 H-413.2 Certification Requirements

(CT:IAH-5; 06-25-2007)

- a. All moderate and high impact unclassified, and all classified systems seeking authorization must have independent certification (see 5 FAM 1065.1-4).
- b. Low impact unclassified systems do not require independent certification but may be certified using resources provided by the sponsoring bureau.
- c. Systems undergoing certification that are connected to the Department must be in compliance with the requirements in 5 FAH-11 H-822.5.
- d. The Certification Package must meet the Department's C&A requirements for system authorization. The sponsoring bureau must verify that:
 - (1) The security controls, put in place to protect the Department's unclassified information and information systems, are in compliance with the requirements in the FIPS Publication 200, the most current version of NIST SP 800-53, 12 FAM 600, 5 FAM, and 12 FAH-6;
 - (2) The security controls, put in place to protect the Department's

classified information and information systems, are in accordance with the requirements in 12 FAM 600 and 12 FAH-6; and

- (3) See the DS/SI/CS and IRM/IA Online Security Resources Library for the most current classified and unclassified security control catalogs. The catalogs map Department and additional national level requirements that must be met in order to comply with the NIST SP 800-53 security controls.

5 FAH-11 H-413.3 Authorization Requirements

(CT:IAH-5; 06-25-2007)

All non-Department systems processing or storing Department information, whether via a connection or not, are required to enter and complete the Non-Department System Authorization Process before DAA authorization is granted.

- (1) New systems must complete the Non-Department System Authorization Process and receive DAA authorization before being allowed to process or store Department information; and
- (2) Systems identified as operating without DAA authorization may be required to cease operations. However, at the discretion of the CIO, and only to meet a critical business need, these systems may be allowed to continue operations, provided the sponsoring bureau makes arrangements with the non-Department entity to begin system authorization of the identified system. Upon identification, authorization must be achieved within three months, or the system may be disconnected.

5 FAH-11 H-413.4 Non-Department System Authorization Process Phases

(CT:IAH-5; 06-25-2007)

Authorization of unclassified non-Department systems progresses through four phases and is similar to the Department's System Authorization Process. The phases include Initiation, Certification, Accreditation, and Life Cycle monitoring. Individuals conducting C&A of a non-Department system must be familiar with all four phases of this process.

5 FAH-11 H-413.4-1 Phase I Initiation Phase

(CT:IAH-5; 06-25-2007)

The sponsoring bureau must, at a minimum, complete and provide the documentation listed in 5 FAH-11 Exhibit H-413.4-1.

5 FAH-11 H-413.4-2 Phase II Certification Phase

(CT:IAH-5; 06-25-2007)

Certification must validate compliance of a system with the minimum mandatory security controls that are defined within the non-Department system's SSP. (See IRM/IA's Web site for the latest minimum mandatory security controls.) The certification requirements (Phase II) are listed in 5 FAH-11 Exhibit H-413.4-2.

5 FAH-11 H-413.4-3 Phase III Accreditation Phase

(CT:IAH-5; 06-25-2007)

Accreditation produces the required evidence to support the Designated Approval Authority (DAA) in making an informed, risk-managed decision to approve or deny authorization of a non-Department system. The risk analyst generates an Authorization Package created during the Certification Phase. Accreditation requirements are in 5 FAH-11 Exhibit H-413.4-3.

5 FAH-11 H-413.4-4 Phase IV Life Cycle Monitoring Phase

(CT:IAH-5; 06-25-2007)

The sponsoring bureau is responsible for audit and continuous monitoring of non-Department systems that it sponsors for authorization. Audits must validate that these systems do not compromise the integrity, availability or confidentiality of Department information systems, or the information processed or stored on behalf of the Department. Life Cycle Monitoring (Phase IV) requirements are in 5 FAH-11 Exhibit H-413.4-4.

5 FAH-11 H-414 PROCEDURE FOR A TARGETED SECURITY CONTROL ASSESSMENT

(CT:IAH-5; 06-25-2007)

- a. A targeted security control assessment (SCA) is performed by the certification analyst to validate whether or not remediated items are successfully mitigated.
- b. A risk analyst reviews the targeted SCA results to determine the level of

residual risk:

- (1) The system may be recommended for full authorization if, after remediation, residual risk is determined to be low; and
 - (2) The system may not be recommended for full authorization until such time that risk is remediated to an acceptable level (low), if remediation is not completed, or remediation did not mitigate unacceptable risk to low.
- c. The DAA can authorize a system with medium and high residual risk. The sponsoring bureau must first make every effort to reduce the risk to low. Next, the sponsoring bureau must send a memorandum to DAA that outlines a supporting business case which demonstrates a critical business need that overrides the security concerns.
- d. Updates to documents that may have been affected by re-entry into an earlier phase of the Non-Department System Authorization Process must be reviewed by the sponsoring bureau to ensure that any changes in the system's baseline, necessary to support re-entry into the process, are accurately recorded.

5 FAH-11 H-415 REACCREDITATION OF NON-DEPARTMENT SYSTEMS

5 FAH-11 H-415.1 General

(CT:IAH-5; 06-25-2007)

- a. Reaccreditation of systems can be event-driven (e.g. upgrades, laws, regulations, directives, instructions or policies that dictate such activity change), or time-driven (e.g., the authorization has expired). Examples include:

- (1) Event-driven can be represented through a significant system change that requires reaccreditation or the system's operating environment changes to the degree that threats formerly rated as low are now significant enough for reaccreditation;

NOTE: A significant change is one that alters the authorized configuration to the degree that reaccreditation must be considered. Adding a new function or application that establishes a new interconnection with other agencies or non-Department entities is an example;

- (2) Time-driven supports OMB Circular A-130 requirements to re-accredit a system every three years; and
- (3) Changes to laws that define the requirements for protecting a system's baseline controls can be either event- or time-driven. (For example, FISMA and other laws and regulations control processing requirements of unclassified and classified national security information and direct that a system's minimum security controls be sufficient to protect the agency's information and information systems commensurate with the sensitivity level and classification of the information processed. The authorization of a system could be affected and must be evaluated for reaccreditation if these laws and regulations change and the changes are significant.)

b. Authorized systems must be reaccredited prior to expiration of their current authorization.

NOTE: The sponsoring bureau should process the system for reaccreditation within three months prior to the expiration date of the system's current authorization to allow time for recertification to occur.

- (1) The sponsoring bureau must validate that the system meets policy, guidelines, and procedures which require and recommend adequate security controls that balance risk and business needs in submitting a non-Department system for reauthorization.
- (2) Reauthorization of this system is dependent upon the outcome of DAA's review of Accreditation Recommendation to approve or deny authorization and the residual risk posed to Department information systems.

c. The DAA authority may take the following actions if reaccreditation cannot be completed before expiration of the system's current authorization:

- (1) Approve an authorization extension until reaccreditation is achieved and the system is authorized to operate;
- (2) Direct that operations cease, and the system be disconnected and removed from the Department's IT asset inventory (ITAB); or
- (3) Accept the risk and authorize the system. In this case, every effort to reduce risk to low must be exhausted, and the sponsoring bureau must demonstrate that a critical business need overrides the security concerns.

d. Sponsoring bureaus must ensure that their sponsored non-Department

unclassified system is compliant with the latest FIPS 200 requirements when submitting a system for reaccreditation. Security control sets must be validated and selected under the Department's latest implemented Security Control Baseline Process and Security Control Catalog for Unclassified Systems. (See 5 FAH-11 H-412.6 b(3) above for security controls for classified systems.)

- e. System reaccreditation begins at the Initiation Phase (Phase I), and progresses through all tasks initially completed during the original accreditation, and ends at the Lifecycle Monitoring Phase (Phase IV).
- f. All phases of the Non-Department System Authorization Process must be successfully completed before a system is once again granted full authorization to process or store Department information.

5 FAH-11 H-415.2 Reaccreditation Of Non-Department Systems Resulting From A Significant Change

(CT:IAH-5; 06-25-2007)

- a. Reaccreditation of a system is required whenever a significant change is made to the accredited system's baseline. Proposed modifications to a system (including software, firmware, hardware, or interfaces and interconnections to networks) must be jointly reviewed by the sponsoring bureau and IRM/IA to determine if the proposed modifications will impact the connecting system's (and subsequently the Department system's) protection profile.
- b. The DAA may extend authorization to continue to process or store information until reaccreditation is completed and full authorization is once again granted in cases where a non-Department system's authorization has expired, or is about to expire but has been submitted for or is undergoing reaccreditation.
- c. The sponsoring bureau must assess the risk in cases where a system is undergoing major modifications. The risk must be lower than moderate to high risk before the system can qualify for an authorization extension.
- d. The sponsoring bureau must submit a memo to the DAA indicating that reaccreditation for the specified system is due at least three months prior to expiration of the system's current authorization, unless circumstances dictate otherwise. A non-Department system must be scheduled for reauthorization upon submittal of the reaccreditation request memo.

5 FAH-11 H-415.3 Reaccreditation Of Non-Department Systems Without Significant Change To Baseline Configuration

(CT:IAH-5; 06-25-2007)

- a. The sponsoring bureau must ensure that the system complies with all applicable Department Security Configuration Guidelines if an authorized system is due for reaccreditation and has not undergone any significant change to its baseline configuration.
- b. The sponsoring bureau should conduct a spot check of the system to ensure the original documentation and evidence, used in the former authorization, still applies. If so, the sponsoring bureau will coordinate their efforts. Accomplish this by:
 - (1) Department-approved application scans of the system;
 - (2) Documentation review (specifically the SSP and CP); and
 - (3) Review of waivers and/or exceptions applied for and granted since authorization of the system.
- c. The sponsoring bureau must review the results of Department-approved scans and system documentation provided by the non-Department system owner for configuration compliance, including the summary status of POA&Ms from the previous assessment. In the event no new vulnerabilities are noted:
 - (1) The current authorization must be amended to reflect no significant changes have occurred, and no new vulnerabilities were found that require remediation action;
 - (2) The system's current authorization date must remain unchanged; and
 - (3) The sponsoring bureau must recommend that the DAA approve reauthorization of the system extending up to three years from expiration date of its current authorization.
- d. If conducting a spot check and it is determined that new vulnerabilities exist because of a significant change in the system's baseline configuration, the non-Department system may be required to undergo re-certification and reaccreditation in Phases I through III before granting reauthorization.
- e. The DAA may require the system to undergo a targeted C&A in

accordance with the requirements in this subchapter if authorization of a moderate or high application is due to expire.

5 FAH-11 H-415.4 Requirements for Addressing Baseline Configuration Changes To Non-Department Systems

(CT:IAH-5; 06-25-2007)

- a. The sponsored non-Department entity must notify the sponsoring bureau prior to implementation of the change if an authorized system is due to undergo a significant change to its baseline configuration.
- b. The sponsoring bureau must ensure that system updates are complete if a system is not authorized but is scheduled for C&A under system authorization. On the other hand, this bureau can instead request that the system remain unchanged in its current baseline configuration before system authorization is allowed to start or continue.
- c. Requested changes to a non-Department system's baseline configuration must be assessed for their impact on the Department's infrastructure (systems operations, and/or security).
 - (1) The non-Department entity must provide the sponsoring bureau a Business Impact Summary, clearly stating the business impact the proposed changes may have to the system. (See IRM/IA's Web site for instructions on preparing this summary.)
 - (2) The assigned independent certification analyst must review the request to confirm whether or not the change is significant enough to warrant reauthorization:
 - (a) A memo from the sponsoring bureau to the non-Department entity must be issued stating reauthorization is not required if the request is not a major change to the baseline;
 - (b) The reauthorization process must continue if the request describes a major change to the baseline; and
 - (c) The independent certification and accreditation team should confer or meet with the sponsoring bureau if further investigation is required to determine if the change is major.
- d. The sponsoring bureau must approve and manage changes to a non-Department system's baseline configuration under strict configuration management requirements. All changes must be promptly recorded in

the system's SSP and CP, where appropriate. Additional security controls which affect a system's security posture must be implemented in accordance with requirements in the Department's Security Control Baseline Process and Security control Catalog For Unclassified Systems.

- e. Unauthorized and/or undocumented changes to the system's accredited baseline configuration may invalidate the system's authorization.
- f. The sponsoring bureau must ensure that changes to a non-Department system are authorized, documented, and registered accordingly.

5 FAH-11 H-416 END OF LIFE CYCLE REQUIREMENTS FOR NON-DEPARTMENT SYSTEMS

5 FAH-11 H-416.1 Criteria For Disposal Of Non-Department Systems

(CT:IAH-5; 06-25-2007)

- a. A system reaching the end of its lifecycle must be disposed of in a secure manner (see 12 FAM 620).
- b. The non-Department entity must generate and forward the request for disposal of the unclassified system to the sponsoring bureau.
- c. The assigned certification analyst and the sponsoring bureau must review the disposal request and timeframe to:
 - (1) Ensure the system is properly scheduled for disconnection from the Department information system;
 - (2) Determine the system is safe to shut down and that safe disposal is coordinated in accordance with Department regulations (See 12 FAM 629);
 - (3) Inform ITAB of the request to retire a system and remove it from the Department's IT asset inventory; and
 - (4) File the request for disposal, and any other documentation confirming the safe disposal, in IRM/IA's documentation library.
- d. The IRM/OPS and the sponsoring bureau must jointly investigate issues of improper system disconnection and disposal, and scheduling of disposal,

ITAB filings or disagreements with a disposal request. IRM/OPS will inform all affected parties of the appropriate actions in consideration for proper disposal of a system in the above instances and in anticipation of a non-Department system's shutdown.

- e. The areas the sponsoring bureau must address before elimination of a system includes, but not limited to the:
 - (1) Archiving of information;
 - (2) Disposal of hardware, firmware, and software; and
 - (3) Sanitization of media.
- f. The sponsoring bureau must accomplish, at a minimum, the following management tasks when a system reaches the end of its lifecycle:
 - (1) Send a memo to ITAB indicating system disposal;
 - (2) Contact ITAB maintenance to update the application status to indicate that the system is submitted for retirement and disposal (including system's disposal date); and
 - (3) Inform bureau staff and affected parties outside the bureau that a retirement application is submitted and pending approval, and that system disposal is imminent.
- g. An extension to accommodate system disposal may be granted for unclassified systems scheduled for retirement and disposal within four months after the expiration date of their authorization. In this event, the sponsoring bureau must:
 - (1) Send the CIO an extension request. The extension request must include a business case that justifies an extension and the conditions under which it is requested.
 - (a) If granted, the system will not need to undergo re-accreditation, but instead will be retired and disposed of as scheduled.
 - (b) If denied, the system must be turned off and disconnected upon expiration of its current authorization and before the actual disposal date; and,
 - (2) Have approved extensions in effect starting upon expiration date of a system's authorization, and remain in effect until system disposal is completed.

- h. Classified systems must be disposed of in accordance with Department guidelines and requirements.

5 FAH-11 H-417 THROUGH H-419 UNASSIGNED

5 FAH-11 EXHIBIT H-413.4-1 PHASE I – INITIATION

(CT:IAH-5; 06-25-2007)

- a. Start the initiation process.
 - (1) Memo request for system authorization activities.
 - (2) A Security Categorization Form, also referred to as IT Asset Categorization form (for more information on how to complete the Security Categorization Form and register a system, refer to the ITAB Web site):
 - (a) If the system is already entered in ITAB, this form will collect the remainder of the necessary information; and
 - (b) If the system is not registered in ITAB, the sponsoring bureau must register it after completing this form.
 - (3) System Security Plan (SSP). All systems seeking authorization under the Non-Department System Authorization Process, whether classified or unclassified, must have a SSP, that, as a minimum:
 - (a) Is current with the system's baseline configuration;
 - (b) Defines the system's baseline security controls; and
 - (c) Accurately reflects the system's accreditation boundary.
 - (4) Contingency Plan (CP). If required, the CP must prescribe how the system is to be recovered to full operation in the event that risk is realized and the system loses its integrity, confidentiality, or availability. Not every system requires a CP. However, based on the system type, systems must have a CP if they support critical Department operations:
 - (a) General Support Systems (GSS) and Major Applications (MA) critical to operations and mission support of the Department's infrastructure;
 - (b) Systems that process sensitive information, including but not limited to, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Federal Managers' Financial Integrity Act (FMFIA), and Privacy Act information; and

- (c) Systems supported by a single server, which in turn support operations critical to the Department or bureau's mission.
- b. Registration in ITAB. For more information on how to register a system's baseline in the ITAB, refer to the [ITAB Web site](#).
- c. The sponsoring bureau must define the system, including its:
 - (1) Support role;
 - (2) Operating environment;
 - (3) Supporting applications (hardware/software configuration); and
 - (4) Boundary of operation.
- d. Once the above (Phase I) requirements are completed, the sponsoring bureau and the assigned IRM/IA personnel, with senior management support from the non-Department entity, jointly develop a project work plan, under the direction of IRM/IA, which formally establishes project milestones and resources necessary to achieve authorization.
- e. The forms and automated tools needed by the sponsoring bureau to complete their components of the authorization process are located on the IRM/IA Web site under "Systems Authorization."
- f. IRM/IA personnel must verify that the sponsoring bureau completed all documentation to required department standards before a system can move from the Initiation Phase (Phase I), to the Certification Phase (Phase II).
- g. Items that may prevent completion of Phase I requirements include, but may not be limited to:
 - (1) Incomplete or insufficient documentation;
 - (2) Scheduling conflicting events that interfere with the SCA;
 - (3) Lack of completion of Phase I milestones planned for certification and accreditation of the system; and
 - (4) Escalated and unresolved issues within the ongoing certification and accreditation process.
- h. Refer to the IRM/IA Web site for more information on (1) asset registration requirements, (2) forms using available automated tools, and (3) the latest Automated CP/SSP Tool Guide for generating system security, and contingency plans.

5 FAH-11 EXHIBIT H-413.4-2 PHASE II – CERTIFICATION

(CT:IAH-5; 06-25-2007)

- a. IRM/IA or the sponsoring bureau must ensure that certification of a non-Department system is accomplished in accordance with Phase II certification requirements, whether performed independently or not. This includes requirements to:
 - (1) Prepare and perform the security control assessment (SCA) discussed in 5 FAH-11 H-414.2;
 - (2) Compile the SCA results (findings); and
 - (3) Generate the Certification Report and notify IRM/IA of its completion at the end of the Certification Phase (Phase II).
- b. To ensure that the system is ready for a SCA, the sponsoring bureau must validate that:
 - (1) Support requirements (time and resources) for its completion will be met; and
 - (2) The system is not undergoing, or is not scheduled to undergo, major changes to its baseline configuration that may interfere with the SCA.
- c. If independent certification of a system is required, and the sponsoring bureau:
 - (1) Requests IRM/IA assistance, the certification analyst, under authority and direction of the CISO, must:
 - (a) Perform a SCA;
 - (b) Compile SCA results (findings); and
 - (c) Generate the Certification Report and notification to the IRM/IA advocate of its completion at the end of the Certification Phase (Phase II); or
 - (2) Does not request IRM/IA assistance, the sponsoring bureau, under authority and direction of CISO, must ensure that:

- (a) The SCA is performed in accordance with the Department's Non-Department System Authorization Process (found in this subchapter);
 - (b) The non-Department entity provides the sponsoring bureau the compiled SCA results (findings), which the sponsoring bureau forwards to IRM/IA for review; and
 - (c) The non-Department entity generates and provides the Certification Report upon completion of the SCA to the sponsoring bureau, who in turn forwards it to IRM/IA upon completion of the Certification Phase (Phase II).
- d. After verifying that the Certification Report is completed in the proper format, it will be released to Risk Management for assignment and analysis.
- e. The risk analyst, assigned by IRM/IA Risk Management to review the Certification Report, must:
- (1) Analyze the SCA findings. If after analysis, the risk analyst determines that issues in the Certification Report need resolving, the process cannot move into the Accreditation Phase (Phase III). All issues with SCA findings must be resolved between the certification analyst and the risk analyst before the process can move to the next phase; and
 - (2) Accept the Certification Report. If after analysis the risk analyst accepts the Certification Report, which is included in the Certification Package, the Certification Phase (Phase II) is formally completed and the Accreditation Phase (Phase III) begins.
- f. If a system does not meet certification requirements for completion of Phase II, the system will not be allowed to move to Phase III until Certification and Risk Management verify and agree that Phase II requirements are met.
- g. Items that may prevent completion of Phase II requirements are similar to the items listed in Phase I.

5 FAH-11 EXHIBIT H-413.4-3 PHASE III – ACCREDITATION

(CT:IAH-5; 06-25-2007)

- a. When generating an Accreditation Report as part of the Authorization Package, a risk analyst must:
 - (1) Characterize the acceptable amount of risk, based on the information provided by the certification results;
 - (2) Provide an analysis of the current nature of threats posed against a system; and
 - (3) Formalize a recommendation to DAA for approval or denial of a system's authorization in an Authorization Memorandum, which is included as part of the Accreditation Report.

- b. The Accreditation Report must be reviewed and cleared in IRM/IA in accordance with internal IRM/IA clearance processes. In the review process, Risk Management must validate that the Accreditation Report:
 - (1) Documents the assessed risk in the final risk assessment;
 - (2) Validates the vulnerabilities identified in Certification;
 - (3) Itemizes estimated costs for recovery and replacement of systems with medium to high risk, (see the Department's IT Cost Estimating Guide);
 - (4) Generates the system's initial POA&M report listing the identified vulnerabilities in the Certification Report, finalized in Phase II; and
 - (5) Substantiates the recommendation to the DAA to approve or deny authorization.

- c. After receiving the Accreditation Report, which must contain Risk Management's authorization recommendation, the DAA will either accept or reject the report based on the residual risk posed to the Department, and/or any documented business needs that may override security concerns:
 - (1) If the DAA determines that issues in Accreditation Report or accompanying Authorization Memorandum need resolving, then the process cannot move forward until all issues are resolved to the

DAA's satisfaction; or

- (2) If the DAA accepts and signs the Authorization Memorandum in the Accreditation Report, it is forwarded from IRM/IA to the sponsoring bureau for signatures.
- d. Once the DAA signs the Authorization Memorandum, the authorization decision is made final, and the process is allowed to move to Phase IV of the process:
- (1) In cases where full authorization is granted and all approving authorities have signed the Accreditation Report (i.e., DAA, CISO, sponsoring bureau, and other designated Key Participants), the Accreditation Phase (Phase III) ends and the Lifecycle Monitoring Phase (Phase IV) begins.
 - (2) In cases of a denial of authorization to operate due to medium or high risk, the CIO may direct operations to cease and the system be disconnected and removed from the Department's IT asset inventory as entered in ITAB.
 - (a) Under special circumstances where a business need overrides security concerns, the DAA may overrule a denial recommendation and accept medium to high risk, in which case authorization may be granted. Prior to this event, the sponsoring bureau must submit a memorandum to IRM/IA that outlines a business case which demonstrates and justifies an overriding business need for operations to continue, and which shows that all efforts to reduce risk have been exhausted. Otherwise, at the discretion of the CIO, operations **will** be discontinued.
 - (b) Upon completion and validation of its remediation, the system that received a denial to operate must be re-entered into and successfully complete system authorization - from Phase I through end of Phase IV - to achieve DAA authorization to operate.
- e. IRM/IA must ensure that original copies of the completed authorization package sent to IRM/IA are scanned and converted to ".pdf" format (Adobe file format) for archival and inspection purposes. Archived documentation (filed in both electronic and written form):
- (1) Validates that system authorization is completed in accordance with Department requirements (this subchapter);
 - (2) Supports OMB audit requirements; and

- (3) Must be maintained throughout the life cycle of the system, until disposal.

5 FAH-11 EXHIBIT H-413.4-4 PHASE IV – LIFE CYCLE MONITORING

(CT:IAH-5; 06-25-2007)

- a. Lifecycle monitoring activities performed by the sponsoring bureau on behalf of systems should include, but are not limited to:
 - (1) System security management;
 - (2) Risk management review;
 - (3) Configuration management and control of information system components (see 5 FAH-5 H-521). The sponsoring bureau must verify with the sponsored non-Department entity that required configuration items exist, and current versions agree with the specified requirements. Examples include:
 - (a) Documentation (specifically the SSP and CP);
 - (b) Source and executable code (changes to and modification of function);
 - (c) Database and test database scripts and associated access privileges;
 - (d) Modification to commercial-off-the-shelf (COTS) and/or patches to COTS products and updates (see below GOTS); and
 - (e) Modification to U.S. Government-off-the-shelf (GOTS) and/or patches to GOTS products and updates;
 - (4) Security impact analysis of changes to the system. This includes integration testing and evaluation of new or modified hardware or software for the enterprise network, as well as, coordination and distribution of new releases of software updates and fixes (patches) and version control;
 - (5) Ongoing assessment of security controls, including but not limited to:
 - (a) Audit logs;
 - (b) User accounts and password settings; and

- (c) System access permissions;
- (6) System security requirements and status reporting; and
- (7) In meeting reporting requirements of annual self-assessments, the sponsoring bureau must:
 - (a) Ensure that the required annual self-assessment is conducted on the systems completing authorization, and ensure that the results are recorded in the systems' SSPs; and
 - (b) Report the self-assessment results to IRM/IA no later than 30 days after completion of the self-assessment.
- b. A Non-Department entity must initiate a new authorization cycle if either (1) major modifications to the site IT Infrastructure or (2) significant changes in threats or operating environment occur. Otherwise, the system undergoes re-accreditation for the term defined in the authorization.
- c. Sponsoring bureaus must use the Department-approved automated tools posted on the IRM/IA Web site to facilitate reporting the self-assessment results of a system to IRM/IA.
- d. For further guidance on management requirements in life-cycle management, see 1 FAM 275.1-3.