FSIS DIRECTIVE

1306.2 Revision1	4/4/16

INFORMATION SYSTEM SECURITY ASSESSMENT AND AUTHORIZATION

I. PURPOSE

This directive lists security assessment and authorization (A&A) requirements as stated in the National Institute of Science and Technology (NIST) Special Publication (SP) 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* and NIST SP, 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* and provides general information concerning how the Office of the Chief Information Officer (OCIO) implements them. This revision updates references and security controls required by the NIST.

II. CANCELLATION

FSIS Directive 1306.2, *Information System Certification and Accreditation (C&A),* 9/28/11

III. BACKGROUND

A. FSIS ensures that information security controls are in place to protect FSIS information systems and data in compliance with Public Law 107-347, Title III, *E-Government Act of 2002*; Public Law 93-579, *Privacy Act of 1974*, as amended; and USDA regulations.

B. Public Law 113-283 was signed into law by the President as the *Federal Information Security Modernization Act of 2014* (FISMA). The goals of FISMA include the development of a comprehensive framework to protect the Government's information, operations, and assets. FISMA assigns specific responsibilities to Federal agencies, and particularly to the NIST and the Office of Management and Budget (OMB), to strengthen information technology (IT) system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information security risks to an acceptable level. All information systems within FSIS require certification and accreditation before they become operational. The certification and accreditation process is a vital component of the overall security program.

C. OCIO certifies and accredits information systems in accordance with NIST SP 800-37, Revision 1, NIST SP, 800-53, Revision 4, Departmental Regulations, and Agency procedures. To adhere to the NIST SP 800-37 and NIST SP 800-53, Revision 4, requirements, FSIS is responsible for meeting the A&A requirements stated in section V. of this directive.

IV. ROLES AND RESPONSIBILITIES

All NIST SP 800-37, Revision 1, and NIST SP, 800-53, Revision 4, requirements in this directive are the responsibility of OCIO unless otherwise stated in this section.

A. **OCIO.**

1. Promotes and supports A&A policy throughout the Agency;

2. Works closely with authorizing officials and their designated representatives to ensure that an Agency wide security program is effectively being implemented;

3. Ensures required A&As are accomplished in a timely and cost-effective manner; and

4. Centralizes reporting of all security-related activities.

B. **Authorizing Official (AO).**

1. Ensures that the operation of an information system creates no more than an acceptable level of risk to Agency operations, assets, or individuals;

2. Is accountable for the risks associated with operating an information system; and

3. Appoints the information system owner.

C. **Certifying Official (CO).**

1. Conducts a 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 with respect to meeting the security requirements for the system;

2. Recommends corrective actions to reduce or eliminate vulnerabilities in the information system;

3. Provides an independent assessment of the information system security plan before initiating the security assessment activities; and

4. Ensures that the plan provides a set of security controls for the information system that adequately meets all applicable security requirements.

D. **System Owners.** System owners may be from program areas outside of OCIO.

1. Determine the procurement, development, integration, modification, or operation and maintenance of an information system;

2. Assist in the development and maintenance of the information system security plan;

3. Ensure the information system is deployed and operated according to the agreed upon security requirements;

4. Ensure system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior);

5. Establish access rights and types of access privileges; and

6. Assist in the development of detailed operating procedures at the system or general support system level that satisfies the A&A security controls.

E. **Information Systems Security Program Manager (ISSPM).**

1. Assist in the certification and accreditation of all Agency IT systems;

2. Participate in Certification Teams providing guidance, testing security controls, and assisting in the preparation of the final A&A package, as required;

3. Monitor and electronically track progress using the Plan of Action and Milestones (POA&M) and the A&A progress on IT systems and report progress to the Agency Chief Information Officer (CIO), including all systems under Authority to Operate (ATO), to ensure that deficiencies are corrected in a timely manner;

4. Identify system changes that require re-accreditation in conjunction with the Agency Technical Change Control Board; and

5. Participate in the preparation of ATO packages, as required.

F. **OCIO Information Systems Security Officer (ISSO).**

1. Serves as the principal technical advisor and is responsible to the CO, information system owner, or ISSPM for ensuring that the appropriate operational security posture is maintained for an information system or program;

2. Maintains the day-to-day security operations of the information systems including:

   a. Physical security;

   b. Personnel security;

   c. Incident handling; and

   d. Security awareness training and education.

3. Provides assistance on an as needed basis to:

   a. Assist in the development of the information system security policy and ensures compliance with that policy on a routine basis;

   b. Work closely with information system owners;

   c. Develop and update information system security plans;

   d. Manage and control changes to information systems; and

   e. Assess the security impact of changes.

V. NIST SP 800-37, REVISION 1 and NIST SP, 800-53, REVISION 4 REQUIREMENTS

A. **Security Assessments.**

1. Develop a security assessment plan that includes the security controls and control enhancements under assessment, the assessment procedures used to determine security control effectiveness and the assessment environment, team, and roles and responsibilities;

2. Assess all information system security controls during the initial security accreditation;

3. Integrate security assessment as a key factor in security authorization decisions and into the information system development life cycle;

4. Conduct the information system security controls assessment annually, or when there is a major change to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system;

5. Use initial or ongoing system authorizations; continuous monitoring; or system development life cycle activities to satisfy annual assessment requirements;

6. Employ an independent assessor or assessment team to conduct the initial and 3-year assessments of the information system security controls;

7. Produce security assessment reports that document the results of the assessment and provide the results in writing to the authorizing official or authorizing official's designated representative; and

8. Provide as part of the security control assessment in-depth monitoring, malicious user testing, penetration testing, and red team exercises. This requirement is only applicable to HIGH systems. The categorization of "HIGH," "MODERATE," or "LOW" is defined in Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*.

B. **System Interconnections.**

1. Authorize all connections from the information system to the other information systems outside of the accreditation boundary through the use of Interconnection Security Agreements;

2. Monitor and control system connections continuously by verifying enforcement of security requirements;

3. Assess risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the Agency and external to the Agency. Risk considerations include information systems sharing the same networks;

4. Document for each connection the interface characteristics, security requirements, and the nature of the information communicated;

5. Review and update Interconnection Security Agreements at least annually; and

6. Employ mechanisms to deny all FSIS employees, contractors, and partners, system access to all external systems unless authorized by Agency exception, inter-agency agreement, and IT Security credential enforcement.

C. **POA&M.**

1. Develop and update the POA&M to guide the correction of deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the information system;

2. Use the Agency's information system for documenting remedial actions (e.g., planning and implementation) to track the POA&M; and

3. Update the existing plan of action and milestones based on findings from the security controls assessments, security impact analyses, and continuous monitoring activities.

D. **Security Authorization.**

1. Authorize the information system for processing before operation;

2. Update the authorization at least every 3 years. or when there is a significant change to the information system; and

3. Ensure security authorization is approved and signed by the Authorizing Official (AO).

E. **Continuous Monitoring.**

1. Monitor the information system security controls. Continuous monitoring activities include:

   a. Configuration management and control of information system components;

   b. Security impact analysis of changes to the information system;

   c. Ongoing assessment of security controls through continuous monitoring strategies;

   d. Regularly reporting on the information system's status with regard to assessment and authorization and continuous monitoring efforts to designated officials; and

   e. Correlate and analyze security-related information generated by assessments and monitoring.

2. Establish the selection criteria and subsequently select a subset of the security controls employed within the information system for annual assessment;

3. Establish the schedule for control monitoring to ensure adequate coverage of security controls and resources is achieved; and

4. Employ an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

F. **Penetration Testing.** Conduct penetration testing annually on Agency-identified scenarios. This requirement is only applicable to HIGH systems.

G. **Internal System Connections.**

1. Authorize internal connections of all information systems; and

2. Document, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated.

VI. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

FSIS Directive 1300.7, *Managing Information Technology (IT) Resources*, sets forth the FSIS policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and

telecommunications equipment. In addition, FSIS Directive 4735.3, *Employee Responsibilities and Conduct*, outlines the disciplinary action that FSIS may take when an employee fails to fulfill responsibilities or adhere to standards of conduct.

VII. QUESTIONS

A. For questions regarding A&A, contact the Agency Information System Security Program at: FSIS_Information_Security@fsis.usda.gov.

B. USDA Departmental directives are located at: http://www.ocio.usda.gov/policy-directives-records-forms and FSIS Directives and Notices are located at: http://www.fsis.usda.gov/wps/portal/fsis/topics/regulations.

Assistant Administrator
Office of Policy and Program Development