UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

# FSIS DIRECTIVE

1306.13
Revision 1

9/1/16

## INFORMATION SYSTEM PLANNING

### I. PURPOSE

This directive lists information system planning requirements for information systems as stated in the National Institute of Science and Technology (NIST) Special Publication (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 1306.13, *Information Systems Planning (PL)*, 10/24/11

### III. BACKGROUND

A. Agency planning requirements are critical to ensuring that information systems are protected. Information technology (IT) security plans are important documents in the overall information system planning process and define the system security features and controls. IT security plans also support the Agency's system life cycle development and are to be updated by OCIO on an ongoing basis in order to accurately reflect the current state of the Agency's information systems.

B. FSIS ensures 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.

C. The President signed Public Law 113-283 into law 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 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.

D. NIST SP 800-53, Revision 4, outlines the controls addressed by information system planning. The selection and employment of appropriate security controls for an information system is an important task that can have major implications on the operations and assets of an organization. To adhere to the NIST SP 800-53, Revision 4, FSIS OCIO has established the requirements stated in section VI. of this directive.

## IV. ROLES AND RESPONSIBILITIES FOR FSIS EMPLOYEES OR OFFICES

A. **FSIS System Owners.** System owners are FSIS employees that are designated by their specific program area and may be from program areas outside of OCIO. They are to:

1. Assist in the development and maintenance of detailed operating procedures to satisfy appropriate information system planning security controls;

2. Assist in the development and maintenance of security plans that provide an overview of system security requirements and a description of planned and in-place security controls;

3. Review and revise security plans annually to address system and organizational changes or problems identified during plan implementation or security control assessments;

4. Conduct a privacy impact assessment on information systems in accordance with OMB Memorandum 03-22;

5. Plan and coordinate security-related activities affecting the information system in order to reduce the impact on organizational operations (e.g., mission, functions, image, and reputation), organizational assets, and individuals.
6. Perform routine security-related activities including, but not limited to, security assessments, audits, system hardware and software maintenance, security certifications, testing, and exercises; and

7. Conduct advance planning and coordination that includes both emergency and non-emergency (routine) situation.

B. **FSIS Privacy Officer.**

1. Ensures privacy policies are posted to FSIS Web sites used by the public;

2. Reviews the Privacy Impact Assessment to identify privacy risks from the information provided; and

3. Collaborates with the systems project manager to address privacy concerns.

C. **System Users.** All employees, to include program areas outside of OCIO, contractors, other Federal agencies, state and local governments, and authorized private organizations or individuals who use FSIS IT resources are to:

1. Be knowledgeable of information system planning and this directive; and

2. Ensure their duties are performed in accordance with this directive.

## V. ROLES AND RESPONSIBILITIES FOR OCIO

A. **OCIO Chief Information Officer.**

1. Supports and promotes information system planning throughout the Agency;

2. Approves detailed plans for the overall security program;

3. Ensures that the Agency head signs the transmittal cover letter attesting to the completeness and correctness of the plans; and

4. Develops and maintains an inventory of all IT systems and determine data sensitivity.

B. **OCIO Information System Security Program Manager (ISSPM).** The ISSPM ensures collaboration among organizational entities and compliance of the information system planning controls. In addition, the ISSPM ensures:

1. OCIO designated officials review and approve security plans;

2. Security plans are aligned with FSIS information system and security architecture;

3. Ensures that all personnel are familiar with annual security plan requirements;

4. Ensures that copies of security plans are maintained in the Agency or staff office;

5. Ensures that all IT systems have adequate security controls based on the sensitivity of data, mission criticality, the value of data in the system, and that controls are documented in a security plan;

6. Development, distribution, and tracking of user rules of behavior acknowledgement forms; and

7. Information system planning policy is reviewed at least annually for compliance with applicable Federal laws, Executive orders, directives, policies, and regulations and appropriate updates added.

## VI. NIST SP 800-53, REVISION 4 REQUIREMENTS FOR OCIO

A. **System Security Plan (SSP).**

1. Develop and implement a security plan that provides an overview of the security requirements for the information system that:

    a. Explicitly defines the authorization boundary for the system;

    b. Describes the operational context of the information system in terms of missions and business processes;

    c. Provides the security categorization of the information system including supporting rationale;

    d. Describes the operational environment for the information system and relationships with or connections to other information systems;

    e. Provides an overview of the security requirements for the system;

    f. Identifies any relevant overlays, if applicable; and

    g. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.

2. Ensure designated FSIS officials review and approve the SSP;

3. Ensure the SSP aligns with FSIS information system architecture and security architecture;
4. Review the SSP annually and revise it to address system and organizational changes or problems identified during plan implementation or security control assessments;

5. Update the SSP to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments;

6. Distribute copies of the SSP and communicate subsequent changes to the plan to authorized system personnel;

7. Protect the SSP from unauthorized disclosure and modification; and

8. Plan and coordinate security-related activities (i.e., security assessments, audits, hardware and software management, patch management, and contingency plan testing) affecting the information system with authorized system personnel before conducting such activities in order to reduce the impact on other organizational entities.

B. **Rules of Behavior.**

1. Establish and make readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;

2. Obtain a signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information;

3. Develop a different set of rules based on user roles and responsibilities (e.g., differentiating between the rules that apply to privileged users and rules that apply to general users). Electronic signatures are acceptable for use in acknowledging rules of behavior;

4. Review and update the rules of behavior annually;

5. Require users who have signed a previous version of the rules of behavior to read and resign when the rules of behavior are revised or updated; and

6. Include in the rules of behavior, explicit restrictions on the use of social media and networking sites and posting organizational information on public websites.

C. **Information Security Architecture.** Develop an information security architecture plan for the information system that:

1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information;

2. Describes how the information security architecture is integrated into and supports the enterprise architecture;

3. Describes any information security assumptions about and dependencies on, external services;

4. Provides a review and update of the information security architecture annually to reflect updates in the enterprise architecture; and

5. Ensures that planned information security architecture changes are reflected in the SSP, the security Concept of Operations (CONOPS), and organizational procurements or acquisitions.

## VII. 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.

## VIII. QUESTIONS

A. For questions regarding information system planning, contact the Agency ISSPM at: FSIS_Information_Security@fsis.usda.gov.

B. USDA Departmental directives are located at: http://www.ocio.usda.gov/policy-directives-records-forms.

C. 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