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

FSIS DIRECTIVE

1306.20
Revision 1

9/6/16

INFORMATION SYSTEM AND SERVICES ACQUISITION

I. PURPOSE

This directive lists information system and services acquisition requirements 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 1306.20, *Information System and Services Acquisition (SA)*, 11/14/11

III. BACKGROUND

A. 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.

B. 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.

C. NIST SP 800-53, Revision 4, outlines the controls for information system and services acquisition. 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 has established the requirements stated in Section VI. of this directive.

IV. ROLES AND RESPONSIBILITIES FOR FSIS EMPLOYEES

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 assist in the development and maintenance of detailed operating procedures to satisfy appropriate information system and services acquisition requirements in Section VI. of this directive.

V. ROLES AND RESPONSIBILITIES FOR OCIO

A. **Chief Information Officer (CIO).** Supports and promotes information system and services acquisition policy and procedures throughout the Agency.

B. **OCIO Information System Security Program Manager (ISSPM).**

1. Ensures collaboration among organizational entities;

2. Ensures compliance of the information system and services acquisition requirements in Section V. of this directive; and

3. Ensures this directive 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. **Allocation of Resources.**

1. Determine the security requirements for the information system in mission or business process planning;

2. Determine, document, and allocate as part of the OCIO capital planning and investment control process, the resources required to protect the information system; and

3. Establish a discrete line item for information security in Agency programming and budgeting documentation.

B. **System Development Life Cycle (SDLC).**

1. Manage the information system using a SDLC methodology that includes information security considerations;

2. Define and document information system security roles and responsibilities throughout the SDLC;

3. Identify individuals having information system security roles and responsibilities; and

4. Integrate the organizational information security risk management process into SDLC activities.

C. **Acquisition Process.**

1. Ensure that security requirements and security specifications, either explicitly or by reference, are included in information system acquisition contracts based on an assessment of risk;

2. Ensure the acquisition contract for the information system and service includes, either explicitly or by reference, the following security requirements, descriptions, and criteria:

   a. Security functional requirements;

   b. Security strength requirements;

   c. Security assurance requirements;

   d. Security-related documentation requirements;

   e. Requirements for protecting security-related documentation;

f. Description of the information system development environment in which the system is intended to operate; and

g. Acceptance criteria.

3. Provide a description of the functional properties (i.e., security capability, functions, or mechanisms) of the security controls to be employed;

4. Provide design and implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design and source code or hardware schematics per the FSIS SDLC Manual;

5. Ensure security configuration settings (i.e., allowed functions, ports, protocols, and services) and security implementation guidance are documented; and

6. Employ only information technology products on the FIPS 201-2 approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

D. **Information System Documentation.**

1. Obtain system administrator documentation for the information system that describes:

a. Securely configuring, installing, and operating the information system;

b. Effectively using the system's security features; and

c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

2. Obtain user documentation for the information system that describes:

a. User-accessible security functions or mechanisms and how to effectively use those security functions or mechanisms;

b. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and

c. User responsibilities in maintaining the security of the system, component, or service.

3. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent (due to the age of the system or lack of support from the vendor or manufacturer) and provide appropriate compensating controls in response;

4. Protect documentation as required, in accordance with the risk management strategy; and

5. Distribute documentation to authorized system personnel.

E. **Security Engineering Principles.** Design and implement information systems using security engineering principles including, but not limited to:

1. Developing layered protections;

2. Establishing sound security policy, architecture, and controls as the foundation for design;

3. Incorporating security into the SDLC;

4. Delineating physical and logical security boundaries;

5. Ensuring system developers and integrators are trained on how to develop secure software;

6. Tailoring security controls to meet organizational and operational needs;

7. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and

8. Reducing risk to acceptable levels, and providing informed risk management decisions.

F. **External Information System Services.**

1. Ensure external information system service providers employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements;

2. Define and document government oversight and user roles and responsibilities with regard to external information system services;

3. Employ processes, methods, and techniques to monitor compliance of the external information system services security controls; and

4. Require providers of external information system services to identify the functions, ports, protocols, and other services required for the use of such services.

G. **Developer Configuration Management.** Requires information system developers and integrators to:

1. Perform configuration management during information system design, development, implementation, and operation;

2. Manage and control changes to the information system;

3. Implement only organization-approved changes;

4. Document approved changes to the information system; and

5. Track security flaws and flaw resolution and report findings to FSIS security operations center.

H. **Developer Security Testing and Evaluation.** Require information system developers and integrators, in consultation with associated security personnel to:

1. Create and implement a security assessment plan;

2. Perform unit integration, system regression testing or evaluation per the FSIS SDLC Manual;

3. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and

4. Provide evidence of the execution of the security assessment plan and the results of the security testing or evaluation.

I. **Supply Chain Protection.** Protect against supply chain threats by identifying, managing, and eliminating vulnerabilities at each phase of the life cycle and using complementary, mutually reinforcing strategies to mitigate risk. 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*.

J. **Trustworthiness.** Require the information system to meet a level of trustworthiness that includes:

1. Security functionality such as the security features or functions employed within the system; and

2. Security assurance which means the grounds for confidence that the security functionality is effective in its application. This is only applicable to HIGH systems.

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 and services acquisitions, contact the FSIS 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