FSIS DIRECTIVE	1306.16 Revision 1	9/20/16

SECURITY ASSURANCE

I. PURPOSE

This directive lists security assurance 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 1306.16, *Information Assurance (IA)*, 6/15/11

III. BACKGROUND

A. Security assurance includes measures that protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authentication, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

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 security assurance. 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 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 security assurance;

2. Access only authorized data necessary to perform assigned responsibilities;

3. Report any suspected or actual computer security incidents;

4. Complete all USDA and FSIS-mandated security training prior to receiving access to FSIS IT resources (e.g., Security Awareness and Privacy training);

5. Agree not to disable, remove, or otherwise alter any security-related technical controls or software on information systems; and

6. Protect information technology systems and data from unauthorized access, use, disruption, modification, destruction, or theft. This includes not sharing passwords with any other person and logging out, locking, or enabling a password-protected screen saver before leaving their workstations.

V. ROLES AND RESPONSIBILITIES FOR OCIO

A. OCIO Chief Information Officer (CIO).

1. Delegates the responsibility for the development and implementation of security assurance to OCIO staff;

2. Develops, implements, and updates the information system security program (ISSP), as necessary, and ensures the ISSP is functioning appropriately, is cost-effective, and risk-based controls are implemented;

3. Ensures FSIS complies with Federal laws, regulations, and directives related to information systems security;

4. Designates an information system security program manager (ISSPM) who will have overall responsibility for the development and implementation of the Agency's ISSP;

5. Ensures security assurance policies, standards, and procedures are implemented within OCIO;

6. Ensures OCIO funding, training, and resources are provided to the OCIO ISSPM to support the FSIS mission;

7. Conducts oversight activities verifying information security programs and controls are implemented and functioning, and provides corrective enforcement mechanisms in instances of non-compliance;

8. Oversees the annual security program self-assessments and ensures periodic independent security program reviews are conducted;

9. Ensures FSIS system users complete the mandatory USDA information security awareness training;

10. Administers a security incident monitoring, response, and reporting program; and

11. Compiles the Agency data and responses for USDA Departmental information security reports, such as the annual and quarterly OMB FISMA report.

B. **OCIO Information System Security Program Manager (ISSPM).** Ensures collaboration among organizational entities and compliance of the security assurance controls. In addition the ISSPM:

1. Delegates and manages the ISSP;

2. Verifies the Agency follows security policies, guidance, procedures, and the information security requirements in this directive and provides corrective actions when these requirements are not adhered to;

3. Provides guidance to system owners and program areas on security issues related to the policies, procedures, and information security requirements in this directive;

4. Collaborates with system owners and program areas on the development of solutions with risks associated with Agency applications against overall confidentiality, integrity, and the availability of those applications;

5. Conducts annual self-assessment and independent security program reviews;

6. Executes all information security responsibilities, as directed by the CIO;

7. Develops and implements an information security performance measurement program to monitor the effectiveness of security controls implemented to protect information systems and data;

8. Follows USDA procedures for implementing, testing, and documenting testing results for all security controls; and

9. Develops and updates the ISSP and ensures OCIO implements and monitors subsequent tactical plans.

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

OCIO is to fulfill the following NIST SP 800-53 Revision 4, requirements:

1. Provide security protection of information systems from unauthorized access, use, disclosure, disruption, modification, or destruction of the information collected or maintained by or on behalf of the Agency;

2. Develop, document, and implement an Agency wide ISSP. The ISSP ensures that security of Agency IT resources:

    a. Is cost-effective;

    b. Reduces information security risks to an acceptable level;

    c. Supports the Agency's mission; and

    d. Is addressed throughout the systems' life cycles.

3. Comply with mandated security requirements (e.g., legislation, Executive Order, Presidential directive, OMB, NIST, and USDA);

4. Ensure information security education, awareness, and training are established and maintained for all employees;

5. Perform controlled self-assessments to identify system vulnerabilities associated with unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;

6. Provide subordinate plans for information security networks, facilities, systems, or groups of information systems;

7. Annually test and evaluate the effectiveness of information security procedures, policies, and practices;

8. Develop a process for planning, implementing, evaluating, and documenting remedial action to address security deficiencies;

9. Establish procedures for detecting, reporting, and responding to security incidents; and

10. Implement contingency plans and procedures ensuring continuity of operations of information 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.

VII. QUESTIONS

A. For questions regarding security assurance, 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