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

FSIS DIRECTIVE

1306.8
Revision 2

8/22/16

SECURITY AWARENESS AND TRAINING

I. PURPOSE

This directive lists security awareness and training (SAT) 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 1306.8, Revision 1, *Security Awareness and Training (SAT),* 12/21/12

III. BACKGROUND

A. SAT is federally mandated and is an essential component of FSIS information assurance objectives. It is critical that all employees, contractors, and partners are aware of and understand the potential information system security threats and risks in their day-to-day operations. With FSIS employees geographically dispersed, there is a great opportunity for potential security risks, which is why all system users need training on security issues.

B. Certain FSIS employees have significant information system security roles and responsibilities that require specialized IT training in order to perform their assigned duties. It is the responsibility of all FSIS employees to take training and use information systems in accordance with training instructions. FSIS is to:

1. Identify those employees; and

2. Determine the appropriate specialized training related to the work that those employees perform.

C. 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.

D. 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, the NIST and the Office of Management and Budget (OMB) in order 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.

E. NIST SP 800-53, Revision 4, outlines the controls addressed by SAT. 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 V. of this directive.

IV. ROLES AND RESPONSIBILITIES

All requirements in this directive are the responsibility of OCIO unless otherwise stated.

A. **OCIO.** Supports and promotes SAT throughout the Agency.

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

1. Ensures collaboration among organizational entities;

2. Serves as the SAT functional lead;

3. Coordinates Agency Information Security and Awareness Training to meet the training requirements of Public Law 100-235, *Computer Security Act of 1987*;

4. Assists system owners in identifying appropriate security training for personnel that have significant information system security roles and responsibilities during the systems development life cycle (SDLC); and

5. Documents and provides appropriate security training to personnel (including system managers, system and network administrators) as identified by the Information System Security Officer.

C. **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 assist in the development and implementation of detailed operating procedures to satisfy appropriate SAT controls in in this directive. They are also to:

1. Assist in the development of detailed operating procedures to satisfy appropriate SAT security controls; and

2. Identify the appropriate security training for system users that have significant information system security roles and responsibilities during the SDLC:

    a. Before authorizing access to the system or performing assigned duties;

    b. When required by system changes; and

    c. Annually provide training for all system users.

D. **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 SAT and this directive;

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

3. Ensure that annual training requirements are met as assigned by OCIO.

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

A. **Security Awareness.**

1. Provide basic security awareness training to all information system users (including managers and senior executives) immediately upon hire prior to obtaining network access and annually thereafter; and

2. Determine the appropriate content of security awareness training based on the specific requirements of FSIS and the information system to which system users have authorized access.

B. **Security Training.**

1. Identify, document, and provide the appropriate security training to system users that have significant information system security roles and responsibilities during the SDLC:

   a. Before authorizing access to the information system or performing assigned duties;

   b. When required by system changes; and

   c. Ensure all FSIS employees, contractors, and partners take security awareness training as an annual requirement.

2. Provide system managers, system and network administrators, and other personnel having access to system-level software with the adequate technical training to perform their assigned duties; and

3. Include security awareness training on recognizing and reporting potential indicators of insider threats.

C. **Security Training Records.**

1. Document and monitor individual information system security training activities including basic security awareness training and specific system security training; and

2. Retain individual training records for at least 1 year after employee separation, or as defined by USDA and the National Archives and Records Administration records management policy.

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 additional information about SAT, contact the FSIS SAT team at the SAT mailbox, SAT@fsis.usda.gov, or the FSIS ISSPM at FSIS_Information_Security@fsis.usda.gov.

B. For additional information about training, access, or crediting questions, contact FSIS AgLearn at FSISAgLearn@fsis.usda.gov or call 1–800–336–3747.

C. For problems with the Computer Security Awareness Training course or AgLearn navigation issues, contact AgLearnHelp@genphysics.com or call 1–866–633–9394.

D. 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