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

FSIS DIRECTIVE

1306.12
Revision 2

8/31/16

INFORMATION SYSTEM SECURITY MAINTENANCE

I. PURPOSE

This directive lists maintenance requirements for information systems security 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 1306.12, Revision 1, *Maintenance (MA)*, 12/13/12

III. BACKGROUND

A. The support and operation of an information system is critical to maintaining security of that system while simultaneously enabling its functionality. Information system support and operation ensures that all hardware and software function as expected through loading and maintaining software, monitoring the installation and updates of hardware and operating system software, as well as fixing any and all software or hardware problems. Support also ensures that only Department-authorized software is installed on the information system for security purposes.

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 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.

D. NIST SP 800-53, Revision 4, outlines the controls addressed by information system security maintenance. 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.

DISTRIBUTION: Electronic; All Field Employees **OPI:** OPPD

IV. ROLES AND RESPONSIBILITIES FOR FSIS EMPLOYEES

A. **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 the information system security maintenance requirements in this directive; and

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

B. **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. System owners are to:

1. Ensure periodic and timely maintenance of information systems;

2. Provide effective controls on tools, techniques, mechanisms, and personnel used to conduct information system maintenance; and

3. Assist in the development and maintenance of detailed operating procedures to satisfy appropriate maintenance of security controls.

V. ROLES AND RESPONSIBILITIES FOR OCIO

A. **OCIO Chief Information Officer.** Supports and promotes information system security maintenance throughout the Agency.

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

1. Ensures and provides system owner training;

2. Ensures collaboration among organizational entities; and

3. Ensures compliance of information system security maintenance controls.

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

A. **Information System Security Maintenance.**

1. Develop, document and disseminate to authorized personnel an information system security maintenance policy that addresses:

    a. Purpose;

    b. Scope;

    c. Roles;

    d. Responsibilities;

   e. Management commitment;

   f. Coordination among organizational entities; and

   g. Compliance.

2. Develop and maintain procedures that facilitate the implementation of the information system security maintenance requirements and associated system information system security maintenance controls; and

3. Review and update the current information system security maintenance requirements and procedures at least annually or when significant changes occur.

B. **Controlled Information System Security Maintenance.**

1. Schedule, perform, document, and review records of information system security maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and organizational requirements;

2. Approve and monitor all maintenance activities to include routine scheduled information system security maintenance and repairs, whether the equipment is serviced onsite, remotely, or moved to another location;

3. Ensure removal of the information system or any of its components from the facility for repair is first approved by an appropriate official;

4. Sanitize equipment to remove all information from associated media, following proper procedure, when the information system or any of its components require offsite information system security maintenance or repairs;

5. Verify proper functionality of all potentially impacted security controls after information system security maintenance is performed; and

6. Maintain information system security maintenance records for the information system to include the:

   a. Date and time of information system security maintenance;

   b. Name of the individual performing the information system security maintenance;

   c. Name of escort, if necessary;

   d. Description of the information system security maintenance performed; and

   e. List of equipment removed or replaced (including identification numbers, if applicable).

7. Employ automated mechanisms to schedule and conduct the information system security maintenance as required, to create up-to-date, accurate, complete, and available records of all information system security maintenance actions. 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*;

C. **Information System Security Maintenance Tools.**

1. Approve, control, and monitor the use of information system security maintenance tools and maintain these tools on an ongoing basis;

2. Inspect all maintenance tools carried into a facility by information system security maintenance personnel for unauthorized modifications;

3. Check all media containing diagnostic and test programs for malicious code before they are used in the information system;

4. For HIGH systems, prevent the unauthorized removal of maintenance equipment as follows:

    a. Verify that there is no organizational information contained on the equipment;

    b. Sanitize or destroy the equipment;

    c. Retain the equipment within the facility; and

    d. Obtain an exemption from a designated organization official explicitly authorizing the removal of the equipment from the facility.

D. **Non-Local Information System Security Maintenance.**

1. Authorize, monitor, and control the use of any non-local information system security maintenance and diagnostic activities;

2. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the system security plan (SSP) for the information system;

3. Employ strong identification and authentication techniques in the establishment of non-local information system security maintenance and diagnostic sessions;

4. Maintain records for all non-local information system security maintenance and diagnostic activities;

5. Terminate all sessions and network connections when non-local information system security maintenance is complete;

6. Document procedures for installation and use of non-local and diagnostic tools in the SSP.

7. For HIGH systems, ensure non-local information system security maintenance and diagnostic services performed on information systems are performed by a provider whose own information system implements a level of security equal to the FSIS information system being serviced, unless the component being serviced is removed and sanitized before service begins and before being reconnected to the system.

E. **Information System Security Maintenance Personnel.**

1. Establish a process for information system security maintenance personnel authorization and maintain a current list of authorized information system security maintenance organizations or personnel;

2. Ensure non-escorted personnel performing information system security maintenance locally or remotely have appropriate access authorizations to the information system allowing access to organizational information. Inappropriate access would result in a compromise of confidentiality, integrity, or availability;

3. Designate organizational personnel with required access authorizations and technical competence to supervise the information system security maintenance activities of personnel who do not possess the required access authorizations;

4. For HIGH systems only:

   a. Prior to initiating information system security maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, ensure all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured. These information system security maintenance personnel are to be escorted and supervised during the performance of the maintenance and diagnostic activities; and

   b. Develop and implement alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system.

F. **Timely Information System Security Maintenance.** Obtain information system security maintenance support and spare parts for all essential information system hardware within 1 day of failure.

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 security maintenance, 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.

Daniel Engeljohn

Assistant Administrator
Office of Policy and Program Development