FSIS DIRECTIVE

1306.3 Revision 2	5/3/16

CONFIGURATION MANAGEMENT OF SECURITY CONTROLS FOR INFORMATION SYSTEMS

I. PURPOSE

This directive lists configuration management (CM) of security controls for information system requirements as stated in the National Institute of Science and Technology (NIST) Special Publication (SP), 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 1306.3, Revision 1, *Configuration Management (CM) of Security Controls for Information Systems*, 12/13/12

III. BACKGROUND

A. CM is a process of reviewing and controlling the components of an Information Technology (IT) system to ensure that they are well defined and cannot be changed without proper justification and full knowledge of the consequences. CM ensures that the hardware, software, communications services, and documentation for a system can be accurately determined at any time.

B. OCIO CM provides the processes, tools, and reports used by the Agency to record and update changes to software systems, processes, and hardware. These changes include information versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices.

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. Public Law 113-283 was signed into law by the President 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. All information systems within FSIS require certification and accreditation before they become operational. The certification and accreditation process is a vital component of the overall security program.

E. NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* outlines the controls addressed by CM. 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 and is responsible for meeting 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 CM throughout the Agency.

B. **OCIO Information System Security Program Manager (ISSPM).** Ensures collaboration among organizational entities and compliance of the CM controls.

C. **OCIO Security Operations Center and Quality Assurance and Policy Branch.**

1. Ensures all maintenance adheres to this directive; and

2. Ensures the integrity of information systems and provides effective controls on the tools, techniques, mechanisms, and personnel used.

D. **FSIS Divisions and Branches.**

1. Assist with supporting and implementing the systems configuration; and

2. Ensure CM processes are implemented and maintained.

E. **FSIS System Owners.** System owners may be from program areas outside of OCIO.

1. Approve change requests prior to submitting them to the Change Control Board (CCB);

2. Identify and eliminate unnecessary ports and services; and

3. Participate in the development of detailed operating procedures to satisfy appropriate CM security controls.

F. **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 CM and the requirements in section V. of this directive; and

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

V. NIST SP 800-53, REVISION 4 REQUIREMENTS

A. Baseline Configuration.

1. Establish, document, and maintain a current baseline configuration of the information system;

2. Ensure the baseline configuration of the information system is consistent with the USDA and FSIS Enterprise Architecture (EA);

3. Update the baseline configuration of the information system as an integral part of information system component installations;

4. Review and update the baseline configuration of the information system:

    a. At least annually;

    b. When required, significant changes, corrective actions, or vulnerabilities that are identified with current baseline are to go through the Agency configuration control board process defined in the CCB directive; and

    c. As an integral part of information system component installations and upgrades.

5. Employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. 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*;

6. Retain older versions of baseline configuration as deemed necessary to support baseline rollback;

7. Issue only FSIS dedicated foreign travel electronic devices (DFTEDs) (i.e., laptops, portable electronic storage devices, smartphones, etc.) to individuals traveling to locations that the organization deems to be of significant risk;

8. Ensure DFTEDs are not connected to the FSIS network upon return from foreign travel or locations that the organization deems to be of significant risk; and

9. Ensure DFTEDs are returned to the Service Desk within 10 business days upon return from foreign travel or significant risk areas.

B. Configuration Change Control.

1. Determine, authorize, document, and control changes to information systems that are configuration controlled;

2. Retain and review records of configuration-controlled changes to the system;

3. Audit activities associated with configuration changes to the information system;

4. Coordinate and provide oversight for configuration change control activities through the Agency or system CCB as defined in the CCB Charter or as needed by change requests;

5. Employ automated mechanisms (on HIGH systems only) that:

    a. Document proposed changes;

    b. Notify appropriate approval authorities;

    c. Highlight approvals not received;

    d. Inhibit change until necessary approvals are received;

    e. Document completed changes; and

    f. Notify authorized designated personnel when approved changes to the information system are completed.

6. Test, validate, and document changes to the information system before implementing the changes on the operational system.

C. **Security Impact Analysis.**

1. Analyze changes to the information system for potential security impacts prior to implementation as part of the change approval process; and

2. Analyze new software for security flaws in a separate test environment before installation in an operational environment. This requirement is only applicable to HIGH systems.

D. **Access Restrictions for Change.**

1. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system;

2. Employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. This requirement is only applicable to HIGH systems;

3. Conduct audits of information system changes at least annually as defined in the System Security Plan (SSP) and when indications so warrant, to determine whether unauthorized changes have occurred. This requirement is only applicable to HIGH systems; and

4. Prevent the installation of software programs as defined in the SSP that are not signed with a certificate that is recognized and approved by the organization. This requirement is only applicable to HIGH systems.

E. **Configuration Settings.**

1. Establish mandatory configuration settings for IT products employed within the information system using baselines from the NIST National Checklist Program (NCP) as modified by the Department. When baselines are not available, contact the vendor for recommendations;

2. Implement configuration settings;

3. Identify, document, and approve exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements;

4. Monitor and control changes to the configuration settings in accordance with organizational policies and procedures;

5. Employ automated mechanisms to centrally manage, apply, and verify configuration settings. This requirement is only applicable to HIGH systems; and

6. Employ automated mechanisms to respond to unauthorized changes to baselines. This requirement is only applicable to HIGH systems.

F. **Least Functionality.**

1. Configure information systems to provide only essential capabilities and specifically prohibit or restrict the use of functions, ports, protocols, or services as defined in the SSP;

2. Review information systems at least monthly to identify and eliminate unnecessary functions, ports, protocols, or services;

3. Employ automated mechanisms to prevent program execution in accordance with the SSP. This requirement is only applicable to HIGH systems;

4. Develop and maintain a defined list of active programs authorized to be executed on the information system as defined in the SSP;

5. Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and

6. Review and update the list of authorized software programs at least annually.

G. **Information System Component Inventory.**

1. Develop, document, and maintain a current inventory of information system components and ownership information that:

   a. Accurately reflects the current information system;

   b. Is consistent with the authorization boundary;

   c. Is at the level of granularity deemed necessary for tracking and reporting;

   d. Includes information deemed necessary to achieve effective property accountability (e.g., item, barcode, manufacturer, type, name, serial number, version number, logical location, configuration, or more at component discretion); and

   e. Is available for review and audit by designated organization officials.

2. Update the information system component inventory as an integral part of component installations, removals, and information system updates;

3. Employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components. This requirement is only applicable to HIGH systems;

4. Employ automated mechanisms at least monthly to detect the addition of unauthorized components and devices into the information system and disable network access by such components and devices or notify designated organizational officials. This requirement is only applicable to HIGH systems;

5. Include in property accountability the following information for information system components. This requirement is only applicable to HIGH systems:

   a. A means for identification by a minimum of position and role; and

   b. Individuals responsible for administering the information system components.

6. Verify that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

H. **CM Plan.** Develop, document, and implement a configuration management plan for the information system that:

1. Addresses roles, responsibilities, and CM processes and procedures;

2. Defines the configuration items for the information system and when in the system development life cycle, places these configuration items under CM; and

3. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

I. **Software Usage Restrictions.**

1. Use software and associated documentation in accordance with contract agreements and copyright laws;

2. Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and

3. Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

J. **User-Installed Software.**

1. Establish policies governing the installation of software by users;

2. Enforce software installation policies through monthly system scans; and

3. Monitor policy compliance at least annually.

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 questions regarding CM, 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