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

FSIS DIRECTIVE	1306.9 Revision 2	4/19/16

SYSTEM AND COMMUNICATION PROTECTION

I. PURPOSE

This directive lists system and communication protection (SC) 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 1306.9, Revision 1, *System and Communication (SC) Protection*, 6/15/12

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. 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) 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.

C. NIST SP 800-53, Revision 4, outlines the controls addressed by SC. 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 is responsible for the ensuring the Agency meets 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. **Chief Information Officer (CIO).** Supports and promotes the importance of SC policy throughout the Agency.

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

1. Ensures collaboration among organizational entities; and

2. Ensures compliance with SC controls.

C. **System Owners.** System owners may be from program areas outside of OCIO. Assist in the development of detailed operating procedures to satisfy appropriate SC security controls as discussed in section V. of this directive.

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 the SC policy and the obligations that go with this section V. of this directive; and

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

V. NIST SP 800-53, REVISION 4 REQUIREMENTS

A. **Application Partitioning.** Ensure the information system separates, physically or logically, user functionality (including user interface services) from information system management functionality.

B. **Security Function Isolation.** 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*. The following applies:

1. Ensure the information system isolates security functions from non-security functions (e.g., partitions or domains), including control of access to and integrity of, the hardware, software, and firmware that perform those security functions;

2. Maintain a separate execution domain (e.g., address space) for each executing process;

3. Employ underlying hardware separation mechanisms to facilitate security function isolation;

4. Isolate critical security functions (i.e., functions enforcing access and information flow control) from both non-security functions and from other security functions;

5. Minimize the number of non-security functions included within the isolation boundary containing security functions;

6. Implement security functions that are largely independent modules that avoid unnecessary interactions between modules; and

7. Implement Security functions that are layered structures minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

C. **Information in Shared Resources.** Prevent unauthorized and unintended information transfer via shared resources.

D. **Denial-of-Service Protection.** Denial-of-service is an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.

1. Ensure the information system protects against or limits the effects of denial-of-service attacks;

2. Restrict the ability of system users to launch denial-of-service attacks against other information systems or networks; and

3. Manage excess capacity, bandwidth, or other redundancies to limit the effects of information flooding types of denial-of-service attacks.

E. **Boundary Protection.**

1. Ensure the information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system;

2. Partition higher-impact information systems into separate physical domains or environments.

NOTE: Apply concepts of managed interface restricting or prohibiting network access in accordance with an organizational assessment of risk. FIPS PUB 199 security categorization guides the selection of appropriate candidates for domain partitioning.

3. Allocate publicly accessible information system components to separate sub-networks with separate physical network interfaces;

4. Prevent public access into the organization's internal networks except as appropriately mediated;

5. Limit the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic;

6. Implement a managed interface (i.e., boundary protection devices in effective security architecture) with any external telecommunication service;

7. Implement appropriate controls to the required protection of the confidentiality and integrity of the information being transmitted;

8. Establish a traffic flow policy for each managed interface;

9. Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;

10. Review exceptions to the traffic flow policy at least annually;

11. Remove traffic flow policy exceptions that are no longer supported by an explicit mission or business need;

12. Deny network traffic by default and allow network traffic by exception;

13. Prevent unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms. This requirement is only applicable to HIGH systems;

14. Prevent remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks;

15. Route all internal communications traffic to external networks though authenticated proxy servers within the managed interfaces of boundary protection devices. This requirement is only applicable to HIGH systems; and

16. Fail to a secure state in the event of an operational failure of a boundary protection device.

F. **Transmission Confidentiality and Integrity.**

1. Ensure the information system protects the confidentiality of transmitted information; and

2. Employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures. This requirement is only applicable to HIGH systems.

G. **Network Disconnect.** Ensure the information system terminates network connection at the end of a session or after 30 minutes of inactivity.

H. **Cryptographic Key Establishment and Management.**

1. Establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures when cryptography is required and employed within the information system; and

2. Maintain availability of information in the event of the loss of cryptographic keys by users. This requirement is only applicable to HIGH systems.

I. **Cryptographic Protection.** Ensure the information system implements cryptographic mechanisms for information requiring cryptographic protection.

J. **Collaborative Computing Devices.** Ensure the information system prohibits remote activation of collaborative computing mechanisms with the exception of Departmental Policy as defined in the System Security Plan and provides an explicit indication of use to the local users.

K. **Public Key Infrastructure Certificates.**

1. Ensure the Agency issues or obtains public key certificates under an appropriate certificate policy from an approved shared service provider; and

2. Establish an Agency certification authority cross-certified with the Federal Bridge Certification Authority at MODERATE assurance or higher, or use certificates from an approved shared service provider.

L. **Mobile Code.**

1. Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and

2. Authorize, monitor, and control the use of mobile code within the information system.

M. **Voice Over Internet Protocol (VoIP).**

1. Establish usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the information system if used maliciously; and

2. Authorize, monitor, and control the use of VoIP within the information system.

N. **Secure Name and Address Resolution Service (Authoritative Source).** Ensure the information system requests and performs data origin authentication and data integrity verification on the name or address resolution responses that the system receives from authoritative sources.

O. **Secure Name and Address Resolution Service (Recursive or Caching Resolver).** Ensure the information system requests and performs data origin authentication and data integrity verification on the name and address resolution responses the system receives from authoritative sources.

P. **Architecture and Provisioning for Name and Address Resolution Service.** Ensure information systems that collectively provide name and address resolution service for an organization are fault tolerant and implement role separation.

Q. **Session Authenticity.** Ensure the information system provides mechanisms to protect the authenticity of communications sessions.

R. **Fail in Known State.** Ensure the information system fails to a secure state for all systemic failures preserving system state information in failure. This requirement is only applicable to HIGH systems.

S. **Protection of Information at Rest.**

1. Ensure the information system protects the confidentiality and integrity of information at rest;

2. Employ cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures; and

3. Employ alternative mechanisms to achieve confidentiality and integrity protections, as appropriate.

T. **Process Isolation.** Ensure the information system maintains a separate execution domain for each executing process.

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 SC, contact the FSIS Information Security Program 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