FSIS DIRECTIVE

1306.7 Revision 2	6/21/16

INFORMATION SYSTEMS PHYSICAL AND ENVIRONMENTAL PROTECTION

I. PURPOSE

This directive lists information systems physical and environmental (PE) protection 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 1306.7, Revision 1, *Information Systems Physical and Environmental (PE) Protection*, 12/13/12

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. 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) 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 PE. 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 established the requirements 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 PE protection throughout the Agency.

B. **OCIO Information System Security Program Manager (ISSPM).** Ensures collaboration among organizational entities and tests the controls for each information system annually to ensure that these controls have been satisfied.

C. **System Owners.** System owners may be from program areas outside of OCIO. They are to assist in the development and implementation of detailed operating procedures to satisfy appropriate PE security controls in 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 PE and the requirements in this directive; and

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

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

A. Physical Access Authorizations.

1. Maintain a list of personnel authorized to access each information system;

2. Maintain a list of personnel authorized to access the computer facility;

3. Designate officials within the organization to review and approve the authorized personnel access list and authorization credentials at least quarterly; and

4. Remove individuals from the facility access list when access is no longer required.

B. Physical Access Control.

1. Control all physical access points to the computer facility including designated publicly accessible areas;

2. Verify individual access authorizations before granting access to the computer facility;

3. Control entry or exit to the facility containing the information system using physical access devices or guards;

4. Control access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;

5. Secure keys, combinations, cipher locks, key pad authentication, and other physical access devices;

6. Inventory physical access devices at least annually;

7. Change combinations:

    a. At least annually;

    b. When combinations have been compromised; or

    c. When individuals are transferred or terminated.

8. Replace keys:

a. When keys are lost; or

b. When individuals are transferred or terminated.

9. Escort and monitor visitor activities when visitors are not visiting a publically accessible area; and

10. Control physical access to the information system independent of the physical access controls for the computer facility. These requirements are 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. **Access Control for Transmission Medium.** Control physical access to information system distribution and transmission lines within organizational facilities using locked wiring cabinets, disconnected or locked spare jacks, and protection of cabling using conduit or cable trays.

D. **Access Control for Output Devices.** Control physical access to information system output devices to prevent unauthorized individuals from observing the output.

E. **Monitoring Physical Access.**

1. Monitor physical access to the information system to detect and respond to physical security incidents;

2. Monitor physical and real time intrusion alarms and surveillance equipment;

3. Review physical access log periodically and investigate apparent security violations or suspicious activities;

4. Coordinate results of reviews and investigations with the organizational incident response capability; and

5. Monitor physical access to the information system in addition to the physical access monitoring of the facility as defined by the agency. This requirement is only applicable to HIGH systems.

F. **Visitor Access Records.**

1. Maintain visitor access records to the computer facility (except for designated publicly accessible areas) in accordance with record retention policies and designate officials within the organization to review the visitor access records daily. Visitor access records must include:

a. Visitor's name, organization, and signature;

b. Form of identification;

c. Date of access;

d. Time of entry and departure; and

e. Purpose of visit.

2. Employ automated mechanisms to facilitate the maintenance and review of visitor access records. This requirement is only applicable to HIGH systems.

G. **Power Equipment and Power Cabling.** Protect information system power equipment and cabling from damage and destruction.

H. **Emergency Shutoff.**

1. Provide the capability of shutting off power to the information system or individual system components in emergency situations;

2. Place emergency shutoff switches or devices located in facilities containing concentrations of information resources in a controlled area accessible only by authorized individuals to facilitate safe and easy access for personnel; and

3. Protect the emergency shutoff from accidental or unauthorized shut off.

I. **Emergency Power.**

1. Provide a short-term uninterruptible power supply for the orderly shutdown of the information system in the event of a primary power source loss; and

2. Provide a long-term alternate power source for maintaining minimally required operational capability in the event of an extended primary power source loss. This is only applicable to HIGH systems.

J. **Emergency Lighting.** Maintain automatic emergency lighting that activates during a power outage or disruption and covers emergency exits and evacuation routes.

K. **Fire Protection.**

1. Employ and maintain fire suppression and detection devices and systems for the information system that are supported by an independent energy source;

2. Employ fire detection devices and systems for information systems that:

   a. Activate automatically and notify the organization and emergency responder in the event of a fire. This requirement is only applicable to HIGH systems;

   b. Provide automatic notification of any activation to the organization and emergency responders. This requirement is only applicable to HIGH systems; and

   c. Employ an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

L. **Temperature and Humidity Controls.** Maintain and monitor temperature and humidity within acceptable levels in the computer facility.

M. **Water Damage Protection.**

1. Protect the information system from water damage caused by broken plumbing lines or other water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel; and

2. Employ automatic mechanisms that protect the information system from water damage in the event of a significant water leak. This requirement is only applicable to HIGH systems.

N. **Delivery and Removal.**

1. Authorize and control information system-related items entering and exiting the computer facility and maintain appropriate records of those items; and

2. Isolate the delivery areas, if possible, from the information system and media libraries to avoid unauthorized physical access.

O. **Alternate Worksites.**

1. Employ appropriate management, operational, and technical information system security controls at alternate worksites;

2. Assess as feasible, the effectiveness of security controls at the alternate work sites; and

3. Provide a means for employees at alternate worksites to communicate with information system security staff in case of security problems.

P. **Location of Information System Components.** This is only applicable to HIGH systems.

1. Position information system components within the computer facility to minimize potential damage from PE hazards and to minimize unauthorized access;

2. Consider the location of the computer facility with regard to PE hazards; and

3. Plan the location of the computer facility where the information system resides with regard to PE hazards. Consider the PE hazards in the facility's risk mitigation strategy for existing computer facilities.

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 PE, contact the Agency Information System 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 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