FSIS DIRECTIVE

1306.19 Revision 1	9/6/16

PERSONNEL SECURITY FOR INFORMATION SYSTEMS

I. PURPOSE

This directive lists personnel security (PS) for information systems 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 1306.19, *Personnel Security (PS) for Information Systems*, 10/24/11

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), to strengthen 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 PS. 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.

IV. ROLES AND RESPONSIBILITIES FOR FSIS EMPLOYEES AND OFFICES

A. **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 are to assist in the development and maintenance of detailed operating procedures to satisfy appropriate PS security controls.

B. **The Office of Human Resources (OHR).** Ensures policies and procedures are developed to satisfy the appropriate PS security controls in coordination with the ISSPM.

C. **Contracting Officer Representative (COR).** In support of the Contracting Officer, is responsible for the technical aspects of the contract and serves as technical liaison with the contractor. The COR is also

responsible for the final inspection and acceptance of all deliverables and such other responsibilities as specified in the contract.

V. ROLES AND RESPONSIBILITIES FOR OCIO

A. OCIO Chief Information Officer (CIO).

1. Acts as the agency Senior Security Officer who is responsible for supporting the strategic requirements of the information system security plan (ISSP);

2. Ensures that adequate funding, training, and resources are provided to the Information System Security Program Manager (ISSPM) to support the Agency mission;

3. Serves as the certification official for Agency security requirements (e.g., annual security plans, FISMA and other formal reporting requirements, waiver requests, and certification of Agency IT Systems); and

4. Designates and submits to USDA Cyber Security staff in writing, the names of the ISSPM and Deputy ISSPM, ensuring that these individuals are permanent members of all system development, telecommunications planning and system development life cycle planning teams.

B. OCIO ISSPM.

1. Supports the review of OCIO positions in coordination with the Office of Human Resources (OHR) in order to assign appropriate risk designations;

2. Ensures personnel screening for system access;

3. Tests the controls for each information system annually to ensure that these controls have been satisfied; and

4. Ensures Information System Security Officers (ISSOs) in OCIO are designated to provide adequate security to business, functional, and operational entities.

C. **FSIS Service Desk.** The single point of contact for managing IT related issues from creation to resolution that uses an Automatic Call Distribution (ACD) system with interactive menus, intelligent routing, and integrated voicemail. The service desk operates 24 hour a day, 7 days a week to field service requests using a centralized incident system of record. The service desk accepts service requests via call processing or user-submitted emails and incidents.

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

A. Position Risk Designation.

1. Assign a risk designation to all system user positions and establish screening criteria for individuals filling those positions;

2. Review and revise position risk designations annually and upon position vacancy or change in position description; and

3. Ensure that position risk designations are consistent with 5 CFR 731.106(a), *Designation of Public Trust Positions and Investigative Requirements,* and OPM policy and guidance.

B. **Personnel Screening.**

1. Screen individuals requiring access to organizational information and information systems before authorizing access;

2. Rescreen individuals according to the FSIS defined list of conditions;

3. Ensure that screening is consistent with:

   a. 5 CFR 731.106 (a);

   b. OPM policy, regulations, and guidance;

   c. Organizational policy, regulations, and guidance;

   d. FIPS PUB 201-2, NIST SP 800-73-4, 800-76-2, and 800-78-4; and

   e. The criteria established for the risk designation of the assigned position.

C. **Personnel Termination.** Upon termination of the individual's employment:

1. Disable information system access immediately upon notification of termination;

2. Terminate or revoke any authenticators or credentials associated with the individual;

3. Conduct exit interviews that include, at a minimum, a discussion of nondisclosure agreements and potential limitations on future employment;

4. Retrieve all organizational information system-related property (e.g., keys, identification cards, and building passes);

5. Ensure appropriate personnel have access to data stored on a departing employee's information system;

6. Notify Service Desk immediately upon notification of termination; and

7. Employ automated mechanisms to notify Service Desk upon termination of an individual. 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 System.*

D. **Personnel Transfer.**

1. Review information systems facilities access authorizations when personnel are reassigned or transferred to other positions within the organization;

2. Initiate required actions including:

a. Returning old and issuing new keys;

b. Issuing identification cards or building passes;

c. Closing old accounts and establishing new accounts;

d. Changing system access authorizations;

e. Providing access to data and accounts created or controlled by the employee at the old work location; and

f. Notifying the Service Desk immediately upon notification of transfer.

E. **Access Agreements.**

1. Complete appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access. Review and update the agreements minimally on a yearly basis. Access agreements include:

   a. Nondisclosure agreements;

   b. Acceptable use agreements;

   c. Rules of behavior; and

   d. Conflict-of-interest agreements. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy.

2. Include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized.

F. **Third-Party Personnel Security.**

1. Establish personnel security requirements, including security roles and responsibilities for third-party providers, and monitor provider compliance. Third-party providers include service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management;

2. Require third-party providers to comply with established organizational personnel security policies and procedures;

3. Document personnel security requirements and explicitly include personnel security requirements in acquisition-related documents; and

4. Require third-party providers to notify the COR of any personnel transfers or terminations of third-party personnel who possess organizational credentials or badges, or who have information system privileges as soon as transfers or terminations are known and submit justification for the replacement request.

G. **Personnel Sanctions.**

1. Employ a formal sanctions process for personnel failing to comply with established information security policies and procedures;

2. Notify the FSIS Privacy Officer and Human Resources Director, immediately when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction; and

3. Ensure that the sanctions process is consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The sanctions process can be included as part of the general personnel policies and procedures.

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 PS, contact the FSIS 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