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

# FSIS DIRECTIVE

1306.10
Revision 2

9/8/16

## INFORMATION SYSTEM ACCESS CONTROL

### I. PURPOSE

This directive lists information system access control (AC) 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 1306.10, Revision 1, *Information System Access Control (AC),* 10/17/12

### 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 development of a comprehensive framework to protect the Government's information, operations, and assets. FISMA assigns specific responsibilities to Federal agencies, the National Institute of Science and Technology (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, *Security and Privacy Controls for Federal Information Systems and Organizations,* outlines the controls addressed by AC. 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 in Section VI. of this directive.

### IV. ROLES AND RESPONSIBILITIES FOR FSIS EMPLOYEES

A. **System Owners**. System owners are FSIS employees who are designated by their specific program area and may be from program areas outside of OCIO. They assist in the development of detailed operating procedures to fulfill the following requirements:

1. Account management;

2. Access enforcement;

3. Information flow enforcement;

4. Separation of duties;

5. Least privilege;

6. Unsuccessful login attempts;

7. System use notification;

8. Concurrent session control;

9. Session lock;

10. Session termination;

11. Supervision and review access control;

12. Permitted actions without identification or authentication; and

13. Automated marking.

B. **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 AC; and

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

C. **Contracting Officer Representatives (COR) and FSIS Supervisors.** CORs and FSIS supervisors may be from other program areas outside of OCIO. They ensure the account creation and deactivation of all assigned employees as follows:

1. For account creation, determines the type of access required and submits the appropriate Footprints ticket to request creation of the account; and

2. For account deactivation, upon determination of employee separation, creates a Footprints ticket for “Employee Separation”. Where possible, this ticket is to be created one week in advance of separation.

## V. ROLES AND RESPONSIBILITIES FOR OCIO

A. **Chief Information Officer (CIO).** Supports and promotes the AC policy throughout FSIS.

B. **Information System Security Program Manager (ISSPM).** Performs the following duties:

1. Ensures and provides system owner training;

2. Ensures collaboration among organizational entities;

3. Oversees creation and use of procedures created by system owners to ensure they include the assignment of specific roles and responsibilities to address each security control;

4. Ensures plan of action and milestones (POA&Ms) are developed and maintained; and

5. Ensures this policy is reviewed at least annually for compliance with applicable Federal laws, Executive orders, directives, policies, and regulations and updated as appropriate.

C. **Network Security Operations Center (SOC).** Detects and blocks unauthorized entities on the network.

D. **Infrastructure Operations Division.** Fulfills the following requirements:

1. Remote access;

2. Wireless access restrictions; and

3. Use of external information systems.

E. **Customer Support Division.** Fulfills access control for portable and mobile device requirements.

F. **System Administrator.** Maintains a multi-user computer system, including a local-area network. The duties include but are not limited to:

1. Adds and configures workstations, servers, and routers;

2. Creates and deactivates domain accounts, local accounts and application or system accounts;

3. Installs system-wide software, performs procedures to prevent the spread of viruses; and

4. Allocates mass storage space.

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

A. **Account Management.**

1. Oversee information system accounts by establishing, activating, modifying, reviewing, disabling, or removing accounts;

2. Review information system accounts every 90 days;

3. Identify information system authorized users and specify rights and privileges;

4. Authorize access to information systems based on intended system usage and a valid need-to-know or need-to-share that is determined by assigned official duties and that satisfies all personnel security criteria;

5. Require proper identification for requests to establish and approve information system accounts;

6. Authorize and monitor the use of guest or anonymous accounts;

7. Remove, disable, or otherwise secure unnecessary accounts (e.g., separated account and applications that are no longer in use) within 72 hours;

8. Notify when system user accounts are terminated or transferred associated accounts removed, disabled, or otherwise secured;

9. Employ automated mechanisms to support the management of information system accounts;

10. Terminate temporary and emergency accounts automatically after 30 days;

11. Disable inactive accounts automatically after 90 days;

12. Employ automated mechanisms by appropriate individuals to audit account creation, modification, disablement, and termination actions;

13. Log out when leaving area where computer is located. 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*;

14. Monitor information system accounts for atypical use and report atypical usage. This requirement is only applicable to HIGH systems; and

15. Disable accounts for users that impose a significant risk to the organization. This requirement is only applicable to HIGH systems.

B. **Access Enforcement.** Enforce assigned authorizations controlling access to the system.

C. **Information Flow Enforcement.**

1. Enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems based on information flow policies; and

2. Implement information flow control enforcement as a basis for flow control decisions using:

   a. Explicit labels on information, source, and destination objects;

   b. Protected processing domains (example: domain type-enforcement); and

   c. Dynamic security policy mechanisms.

D. **Separation of Duties.**

1. Enforce separation of duties through assigned access authorizations; and

2. Establish appropriate divisions of responsibility and separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

E. **Least Privilege.**

1. Enforce the most restrictive set of rights or privileges or access needed by system users (or processes acting on behalf of system users) for the performance of specified tasks;

2. Employ the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals;

3. Authorize access explicitly to the list of functions defined in the system security plan (SSP) based on role;

4. Require users of information system accounts, or roles, with access to the security functions defined in the SSP, to use non-privileged accounts, or roles, when accessing other system functions. If feasible, audit any use of privileged accounts, or roles, for such functions;

5. Restrict privileged accounts on the information system to system administrators and power users identified in the SSP;

6. Authorize network access to privileged commands for operational needs as identified in the SSP;.

7. Audit the use of privileged functions to identify misuse, or unauthorized use of the system; and

8. Prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards or countermeasures.

F. **Unsuccessful Login Attempts.**

1. Enforce a policy of five maximum consecutive invalid access attempts by a system user during a 15-minute time period; and

2. Lock the account automatically after the maximum number of unsuccessful attempts has been exceeded for a minimum of 15 minutes unless released by an administrator.

G. **System Use Notification.** Display an approved system user notification message before granting system access informing potential users that:

1. They are accessing a U.S. Government information system;

2. System usage may be monitored, recorded, and subject to criminal and civil penalties;

3. Use of the system indicates consent to monitoring and recording;

4. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and

5. Notification message remains on the screen until user acknowledges the usage conditions and takes specific actions to further access the system.

H. **Concurrent Session Control.** Limit the number of concurrent sessions for any user to one. This requirement is only applicable to HIGH systems.

I. **Session Lock.**

1. Prevent system access by initiating a session lock after 15 minutes of inactivity;

2. Ensure session lock remains in effect until the user re-establishes access using appropriate identification and authentication procedures;

3. Initiate session lock when leaving the information system unattended; and

4. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

J. **Session Termination.** Automatically terminate a user session after 30 minutes of inactivity.

K. **Permitted Actions Without Identification or Authentication.**

1. Identify a document-specific (i.e., security plan) user action that can be performed on the information system without identification or authentication;

2. Document and provide supporting rationale in the security plan for the information system, user actions not requiring identification or authentication; and

3. Permit actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

L. **Remote Access.**

1. Document allowed methods of remote access to information systems;

2. Establish usage restrictions and implementation guidance for each allowed remote access method;

3. Monitor for unauthorized remote access to the information system;

4. Authorize remote access to the information system prior to the connection;

5. Enforce requirements for remote connections to the information system;

6. Employ automated mechanisms facilitating monitoring and control of remote access methods;

7. Use cryptography to protect confidentiality and integrity of remote access sessions;

8. Control remote access through a limited number of managed access control points;

9. Authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and document the rationale for such access in the SSP for the information system;

10. Ensure that remote sessions for accessing security functions as defined in the SSP employ 2-Factor Authentication. All remote session activity for both regular and security related functions is to be audited;

11. Disable Department or Agency restricted network protocols (e.g., Rlogin, and any other Agency-defined non-secure protocols as defined in the SSP), except for explicitly identified components in support of specific operational requirements; and

12. Route all remote accesses through approved USDA and FSIS managed access control points.

M. **Wireless Access.**

1. Establish usage restrictions, configuration or connection requirements, and implementation guidance for wireless access;

2. Monitor for unauthorized wireless access to information systems;

3. Authorize wireless access to the information system prior to connection;

4. Enforce requirements for wireless connections to the information system;

5. Use authentication and encryption to protect wireless access to information systems;

6. Scan for unauthorized wireless access points monthly. Take appropriate action if such access points are discovered. This requirement is only applicable to HIGH systems;

7. Restrict users from independently configured wireless networking capabilities. This requirement is only applicable to HIGH systems; and

8. Confine wireless communications to organization-controlled boundaries. This requirement is only applicable to HIGH systems.

N. **Access Control for Mobile Devices.**

1. Establish usage restrictions and implementation guidance for organization-controlled mobile devices;

2. Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to information systems;

3. Monitor for unauthorized connections of mobile devices to information systems;

4. Enforce requirements for the connection of mobile devices to information systems;

5. Disable information system functionality that provides the capability for automatic execution of code on mobile devices without user direction (e.g., Issue specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with Agency policies and procedures);

6. Apply enhanced analysis and cleaning measures to mobile devices returning from locations that the organization deems to be of significant risk in accordance with Agency policies and procedures;

7. Protect information residing on mobile devices by employing cryptographic mechanisms to provide confidentiality and integrity protection, during storage, and in locked containers while in transit outside of controlled areas; and

8. Only allow mobile device access to information systems in accordance with Agency security guidelines.

O. **Use of External Information Systems.**

1. Establish terms and conditions for authorized individuals to access information systems from an external information system and process, store, or transmit controlled information using an external information system;

2. Prohibit unauthorized individuals from using an external information system to access the information system or to process, store, or transmit controlled information, except in situations where the Agency:

   a. Can verify the employment of required security controls on the external system as specified in the information security policy and SSP; and

   b. Has approved information system connection or processing agreements with the entity hosting the external information system.

3. Limit the use of FSIS-controlled portable storage devices and media by authorized individuals on external information systems.

P. **Information Sharing.**

1. Facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information in accordance with written authorizations, rules of behavior that are to be maintained by the connecting system, service level agreements, interconnection security agreements, and memoranda of understanding, where appropriate; and

2. Employ automated mechanisms or manual processes to assist users in making information sharing and collaboration decisions.

Q. **Publicly Accessible Content.**

1. Designate individuals authorized to post information into the information system that is publicly accessible;

2. Train authorized individuals to ensure that publicly accessible information does not contain non-public information;

3. Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the information system;

4. Review the content on the publicly accessible information system for nonpublic information at least quarterly; and

5. Remove nonpublic information from the publicly accessible information system, if discovered.

## 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 AC, 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