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

FSIS DIRECTIVE

1306.11
Revision 2

9/1/16

INFORMATION SYSTEMS AUDIT AND ACCOUNTABILITY

I. PURPOSE

This directive lists information systems audit and accountability (AU) 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 1306.11, Revision 1, *Information Systems Audit and Accountability (AU)*, 12/13/12

III. BACKGROUND

A. An audit is an independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures. Accountability is the principle that an individual is entrusted to safeguard and control equipment, keying material, and information, and is answerable to proper authority for the loss or misuse of that equipment or information.

B. 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.

C. 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.

D. NIST SP 800-53, Revision 4, outlines the controls addressed by AU. 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

A. **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 AU and the obligations that go with the requirements in this directive; and

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

B. **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 assist in the development and implementation of detailed operating procedures to satisfy appropriate AU security requirements in this directive.

V. ROLES AND RESPONSIBILITIES FOR OCIO

A. **Chief Information Officer (CIO).** Supports and promotes the importance of AU throughout the Agency.

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

1. Ensures and provides system owner training;

2. Ensures collaboration among organizational entities; and

3. Monitors and electronically tracks program actions and milestones (POA&Ms) to ensure that any deficiencies are corrected in a timely manner.

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

A. **Audit Events.**

1. Determine, based on a risk assessment and mission or business needs, that the information system is capable of auditing the following events:

    a. Account login events;

    b. Object access; and

    c. Account creation or deletion information;

2. Coordinate the security audit function with other organization entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

3. Provide a rationale for why the list of auditable events is adequate to support after-the-fact investigations of security incidents;

4. Determine based on current threat information and ongoing assessment of risk, that all events defined as “Auditable Events” be audited according to a schedule defined by the Agency or in the system security plan (SSP); and

5. Periodically (at least annually) review and update the list of organization-defined auditable events.

B. **Content of Audit Records.**

1. Produce audit records that contain sufficient information to establish:

    a. The events that occurred;

    b. The source of the events; and

    c. The outcome of the events.

2. Audit record content is to include:

    a. The date and time of the event;

    b. The component of the information system (e.g., software component, hardware component) where the event occurred;

    c. The type of event;

    d. The user or subject identity; and

    e. The outcome (success or failure) of the event.

3. Provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, and subject; and

4. Provide the capability to centrally manage the content of audit records generated by individual components throughout the system. 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. **Audit Storage Capacity.**

1. Allocate sufficient audit record storage capacity; and

2. Configure auditing to reduce the likelihood of storage capacity being exceeded. The auditing and the online audit processing requirements are to be taken into account.

D. **Response to Audit Processing Failures.**

1. Ensure information systems alert the appropriate officials in the event of an audit processing failure and take appropriate action as defined by policy, procedure, and system-specific requirements (e.g., shut down information system, overwrite oldest audit records, or stop generating audit records);

2. Audit processing failures may be due, but are not limited to, the following:

    a. Software and hardware errors;

    b. Failures in the audit capturing mechanisms;

c. Audit storage capacity being reached or exceeded;

3. Provide a warning when allocated audit record storage volume reaches the level of maximum capacity as defined by policy or procedure. This requirement is only applicable to HIGH systems; and

4. Provide a real-time alert when the specific audit failure events defined by policy or procedure for real-time alerts occur. This requirement is only applicable to HIGH systems.

E. **Audit Review, Analysis, and Reporting.**

1. Review and analyze information system audit records at least weekly or as defined in the SSP for indications of inappropriate or unusual activity;

2. Investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions;

3. Adjust the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to organizational operations, organizational assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information;

4. Analyze and correlate audit records across different repositories to gain organization wide situational awareness;

5. For High systems only:

a. Employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities;

b. Integrate analysis of audit records with analysis of vulnerability scanning information; performance data; information system monitoring information to further enhance the ability to identify inappropriate or unusual activity; and

c. Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

F. **Audit Reduction and Report Generation.**

1. Ensure information systems provide an audit reduction and report generation capability;

2. Ensure audit reduction, review, and reporting tools support on-demand audit review and after-the-fact investigations of security incidents without altering original audit records; and

3. Ensure information systems have the capability to automatically process audit records for events of interest based upon selectable event criteria.

G. **Time Stamps.**

1. Provide time stamps for use in audit record generation;

2. Generate time stamps (including date and time) of audit records using internal system clocks; and

3. Compare and synchronize internal information system clocks on a regular basis, in accordance with policy and procedure.

H. **Protection of Audit Information.**

1. Protect audit information and audit tools from unauthorized access, modification, and deletion;

2. Authorize access to management of audit functionality to only identified privileged users;

3. Back up audit records (e.g., assignment: organization-defined frequency) onto a physically different system or system component than the system or component being audited. This requirement is only applicable to HIGH systems; and

4. Implement cryptographic mechanisms to protect the integrity of audit information and audit tools. This requirement is only applicable to HIGH systems.

I. **Non-Repudiation.** Ensure the information system provides the capability to determine whether a given individual took a particular action. An action by an individual may include creating information, sending a message, or approving information (e.g., indicating concurrence, signing a contract, and receiving a message). This requirement is only applicable to HIGH systems.

J. **Audit Record Retention.** Retain audit records in accordance with FSIS Records Retention and Disposition Schedules (e-Auth login is required to access this information) to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

K. **Audit Generation.**

1. Provide audit record generation capability for the list of auditable events defined in Auditable Events for information system components capable of creating audit records or as defined in the SSP;

2. Allow designated personnel to select which auditable events are to be audited by specific components of the system;

3. Generate audit records for the list of defined audited events with sufficient information establish in the content;

4. Compile audit records from all system components capable of creating audit records or as defined in the SSP into a system-wide (logical or physical) audit trail that is time-correlated to within a maximum of 500ms time deviation from the same Network Time Protocol (NTP) central time source. This requirement is only applicable to HIGH systems; and

5. Provide the capability for designated personnel to change the auditing to be performed on all system components based on an identified threat within the incident category timeframes identified in Department policy. This requirement is only applicable to HIGH systems

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 AU, 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.

D. For additional information regarding records management please contact the Office of Administrative Services, Records Management Staff at RecordsandMail@fsis.usda.gov.

Assistant Administrator
Office of Policy and Program Development