FSIS DIRECTIVE

1306.1 Revision 2	6/9/16

INFORMATION SYSTEM INCIDENT RESPONSE

I. PURPOSE

This directive lists information system incident response (ISIR) 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 1306.1, Revision 1, *Incident Response (IR)*, 8/21/12

III. BACKGROUND

A. ISIR requirements are critical to ensuring that Agency information systems are protected. An ISIR security plan is to be in place to ensure that the proper procedures are followed in the event of any security incident or alleged incident. An ISIR security plan is to be updated on an ongoing basis to reflect changes to the Agency's processes for combating emerging threats in the dynamic security environment.

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 ISIR. 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. **Agency Administrator.** Appoints the appropriate personnel to ensure that information security and privacy policies, procedures, and practices are adequate and in place.

B. **FSIS Assistant Administrators.** Ensure that all incident procedures are followed and that ISIR is accomplished through the Information System Security Program Manager (ISSPM) or the designated incident commander for all incidents.

C. **OCIO.** The Chief Information Officer (CIO), Deputy CIO, and Information System Security Program Manager (ISSPM) promote and support:

1. The importance of ISIR through the Information System Security Program and the Agency; and

2. An effective ISIR.

D. **OCIO ISSPM.**

1. Ensures collaboration among organizational entities on ISIR between the various branches and groups within the Agency and coordinates and adequately responds to IT security incidents;

2. Notifies USDA cyber security of incident resolution status and closure within the specified timeframes; and

3. Certifies the accuracy of incident reports and ensures that an individual has been appointed to lead and coordinate security ISIR for each incident. For the Agency, this individual is the Security Operations Center (SOC) lead.

E. **FSIS Privacy Officer.**

1. Is the authority for directing the identification of Personally Identifiable Information (PII) and the level of impact or sensitivity of compromised PII;

2. Provides direction and guidance concerning PII incidents; and

3. Provides recommendations on the closure of all significant or sensitive PII incidents.

F. **Associate Chief Information Officer (CIO).** Maintains the Agency network and IT assets and provides a coordinated response to security incidents to the ISSPM.

G. **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 ISIR and this directive; and

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

H. **OCIO SOC.** The OCIO SOC processes all computer security events, incidents, and PII compromises that affect the network and users at FSIS. The OCIO SOC is the central point of contact (POC), liaison, and facilitator, which reports all FSIS incidents and events to the USDA Agriculture Security Operations Center (ASOC) Computer Incident Response Team (CIRT). The OCIO SOC complies with the ASOC for the purpose of handling and mitigating incidents.

I. **FSIS Service Desk.** The single point of contact (POC) 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. It operates 24 hour a day, 7 days a week to answer field service requests using a centralized incident system of record. Service requests can be fielded via call processing or user-submitted emails and incidents.

V. GENERAL INFORMATION FOR SECURITY INCIDENTS

A. System Users should immediately call the Agency service desk at 800–473–9135 to report all security incidents.

B. System users that suspect or identify an incident should stop using the workstation, unplug the network connection (if possible) but do not shut down or disconnect power. Then immediately notify their supervisor and the Agency ISSPM at FSIS_Information_Security@fsis.usda.gov.

NOTE: Some examples of general information security incidents include malware (i.e., virus) infection, receipt of inappropriate material via email (e.g., pornography) and unauthorized individuals asking questions about sensitive information.

C. **Incidents Involving Loss or Theft.** Loss or theft of IT resources and media (e.g., laptops, personal digital assistants, hard disks, floppy disks, and CD-ROMs), removable drives (e.g., USB drives, thumb drives), and DVDs are to be reported in the following order:

1. USDA service desk at 888–926–2373, 24 hours a day; and

2. Agency service desk at 800–473–9135, 24 hours a day.

D. **PII Incidents.** A situation involving or suspected to involve PII must be reported immediately to USDA at 877–744–2968 or 888–926–2373, 24 hours a day. This information can also be viewed on the USDA website.

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

A. **ISIR Training.**

1. Provide ISIR training to information system users consistent with assigned roles and responsibilities upon assignment to an ISIR role or responsibility when required by system changes and annually thereafter;

2. Incorporate simulated events into training to facilitate an effective response by personnel in crisis situations. This 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*; and

3. Employ automated mechanisms to provide a more thorough and realistic ISIR training environment. This requirement is only applicable to HIGH systems.

B. **ISIR Testing.**

1. Test the ISIR capability for the information annually using at least, tabletop exercises, to determine the ISIR effectiveness and document the results; and

2. Coordinate ISIR testing with organizational elements responsible for related plans.

C. **Incident Handling.**

1. Acknowledge and respond to all USDA IT security incidents in accordance with the stipulated timeframes and procedures in Department Regulation (DR) 3505-005, *Cyber Security Incident Management Policy*;

2. Implement a protocol for handling security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

NOTE: Incident-related information can be obtained from a variety of sources, including, but not limited to: audit monitoring, network monitoring, physical access monitoring, and user or administrator reports.

3. Coordinate incident handling activities with contingency planning activities;

4. Incorporate the lessons learned from ongoing incident handling activities into the ISIR procedures, training, and testing or exercises and implement the procedures accordingly;

5. Employ automated mechanisms to support the incident handling process; and

6. Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. This requirement is only applicable to HIGH systems.

D. **Incident Monitoring.**

1. Track and document information system security incidents on an ongoing basis; and

2. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information. This requirement is only applicable to HIGH systems.

E. **Incident Reporting.**

1. Ensure that the types of incident information reported, the content and timeliness of the reports are consistent with USDA policy, applicable laws, executive orders, directives, policies, regulations, standards, and guidance;

2. Provide the list of designated reporting authorities or organizations;

3. Employ automated mechanisms to assist in the reporting of security incidents; and

4. Document and report the weaknesses and vulnerabilities in an information system to the appropriate organizational officials as soon as they are identified to prevent security incidents.

F. **ISIR Assistance.**

1. Provide an ISIR support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and

2. Employ automated mechanisms to increase the availability of ISIR-related information and support.

G. **ISIR Plan.**

1. Develop an ISIR plan that:

a. Provides the organization with a roadmap for implementing ISIR capability;

b. Describes the structure and organization of the ISIR capability;

c. Provides a high-level approach for how the IR capability fits into the overall organization;

d. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

e. Defines reportable incidents;

f. Provides metrics for measuring the ISIR capability within the organization;

g. Defines the resources and management support needed to effectively maintain and mature an ISIR capability; and

h. Is reviewed and approved by designated officials within the organization.

2. Distribute copies of the ISIR plan to key personnel identified in the ISIR Plan and complete the following actions:

a. Review the ISIR Plan at least annually;

b. Revise the ISIR Plan to address system or organizational changes or problems encountered during plan implementation, execution, or testing;

c. Communicate ISIR plan changes to key personnel identified in the ISIR Plan; and

d. Protect the ISIR plan from unauthorized disclosure and modification.

VII. CONTACTS WITH EXTERNAL GROUPS AND LAW ENFORCEMENT

When necessary, the Agency works with other Federal, state, and local law enforcement and other USDA components and governmental entities as appropriate and lawful, in order to properly respond to information security incidents.

VIII. 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.

IX. QUESTIONS

A. For questions regarding ISIR, 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. The Agency follows the Agricultures Security Operations Center (ASOC) Computer Incident Response Team (CIRT), *Standard Operating Procedure* (SOP*) for Reporting Security and Personally Identifiable Information Incidents,* when responding to all security incidents. More specific Agency SOPs are developed for incident handling and are to adhere to USDA procedures.

Assistant Administrator
Office of Policy and Program Development