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

FSIS DIRECTIVE	1306.4 Revision1	4/14/16

INFORMATION SECURITY RISK ASSESSMENT

I. PURPOSE

This directive lists Information Security Risk Assessment (ISRA) 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 1306.4, *Risk Assessment (RA),* 6/11/10

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. Public Law 113-283 was signed into law by the President 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 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. All information systems within FSIS require certification and accreditation before they become operational. The certification and accreditation process is a vital component of the overall security program.

C. OCIO certifies and accredits information systems in accordance with NIST SP, 800-53, Revision 4, Departmental Regulations, and Agency procedures. To adhere to the NIST SP 800-53, Revision 4, requirements, FSIS is responsible for meeting the ISRA 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 in this section.

A. **The Chief Information Officer (CIO).** The CIO supports and promotes the ISRA policy throughout the Agency.

B. **OCIO Information System Security Program Manager (ISSPM).** Ensures compliance of the information security ISRA controls and collaborates among organizational entities.

DISTRIBUTION: Electronic; All Field Employees **OPI:** OPPD

C. **System Owners.** System owners may be from program areas outside of OCIO. They assist in the development of detailed operating procedures to satisfy appropriate ISRA security controls.

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 be knowledgeable of the ISRA policy and the obligations that go with this policy. They are to ensure their duties are performed in accordance with this policy.

V. NIST SP 800-53, REVISION 4 REQUIREMENTS

A. Security Categorization.

1. Categorize the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance, and document the results (including supporting rationale) in the system security plan;

2. Document the security categorization results (including supporting rationale) in the System Security Plan for the information system;

3. Review and approve the security categorizations by the designated senior-level officials;

4. Conduct Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems* security categorizations as an agency-wide activity with the involvement of the CIO, senior Agency information security officer, information system owners, and information owners; and

5. Determine potential impacts to other agencies and potential National-level impact in categorizing information systems.

B. Information Security Risk Assessment.

1. Conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the Agency (including information and information systems managed or operated by external parties);

2. Assess risk posed to Agency operations, assets, or individuals from external parties;

3. Document ISRA results in the security plan, risk assessment report, and the Department’s official FISMA reporting tool;

4. Review ISRA results at least annually;

5. Update the ISRA report at least annually or when any significant changes are made to the system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system; and

6. Disseminate ISRA results to designated personnel.

C. **Vulnerability Scanning.**

1. Scan for vulnerabilities in the information system and hosted applications monthly and when significant new vulnerabilities that potentially affect the system are identified and reported;

2. Employ vulnerability scanning tools that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

   a. Enumerating platforms, software flaws, and improper configurations;

   b. Formatting and making transparent, checklists, and test procedures; and

   c. Measuring vulnerability impact.

3. Analyze vulnerability scan reports and results from security control assessments;

4. Remediate legitimate vulnerabilities within 30 days for HIGH risk and 90 days for MODERATE risk; LOW risk shall be remediated in accordance with an organizational assessment of risk. The categorization of "HIGH," "MODERATE," or "LOW" is defined in FIPS PUB 199;

5. Share information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (e.g., systemic weaknesses or deficiencies);

6. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned;

7. Update the list of information system vulnerabilities scanned using an automated check performed daily, or when significant new vulnerabilities are identified and reported;

8. Include privileged access authorization to system components identified in the security plan for selected vulnerability scanning activities to facilitate more thorough scanning; and

9. Determine what information about the information system is discoverable by adversaries and notify appropriate personnel, remove designated information, or change the information system to make designated information less relevant or attractive to adversaries. This requirement is only applicable to HIGH systems.

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 ISRA, 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.

Daniel Engeljohn

Assistant Administrator
Office of Policy and Program Development