FSIS DIRECTIVE

1306.6 Revision 2	6/21/16

SYSTEM AND INFORMATION INTEGRITY

I. PURPOSE

This directive lists the system and information integrity 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 1306.6, Revision 1, *System and Information Integrity (SI),* 12/21/12

III. BACKGROUND

A. System and information integrity is the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

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 development of a comprehensive framework to protect the Government's information, operations, and assets. FISMA assigns specific responsibilities to Federal agencies, 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 system and information integrity. 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 established 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. **OCIO.** Supports and promotes system and information integrity throughout the Agency.

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

1. Ensures collaboration among organizational entities;

2. Ensures all maintenance adheres to system and information integrity requirements;

3. Ensures system and information integrity of information systems; and

4. Provides effective controls on the tools, techniques, mechanisms, and personnel used.

C. **System Owners.** System owners may be from program areas outside of OCIO. They assist in the development and implementation of detailed operating procedures to satisfy appropriate system and information integrity requirements in this directive.

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:

1. Be knowledgeable of system and information integrity;

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

3. Ensure laptop and desktop computers approved for use on the FSIS network are:

    a. Connected to the FSIS network for a time period of at least 60 minutes or sufficient to install information system security patches, software updates, and scanning once every three days; and

NOTE: Connecting to the FSIS network means either physically connecting when onsite at USDA, FSIS facilities or, if offsite, using the FSIS VPN client software.

    b. Restarted once every three days.

V. NIST SP, 800-53, REVISION 4 REQUIREMENTS FOR FSIS SYSTEM USERS

Security Alerts, Advisories and Directives for System Users. The following instructions are for individual system users using their individual computers. For system users utilizing a shared computer, security patches are by computer and not by individual profile. Once the computer has received the patches, other users will NOT have to repeat the process. All FSIS personnel who are assigned FSIS computers and have access to FSIS systems are to:

1. Receive, issue, and take appropriate action in response to information system security alerts, advisories, and directives received from the Team US-CERT, OMB, and USDA;

2. Connect to the network at least once every three days to receive software updates. Local area network (LAN) users are to connect for at least an hour total and virtual private network (VPN) users are to connect for at least 3 hours total;

3. Reboot (restart) the computer after the security patch downloads have completed to allow the downloaded patches to completely install. The following instructions apply:

    a. A pop-up notification will appear once the patches have been applied and the system reboot is ready;

b. Do not turn off computer while being updated. Users may receive a message not to turn off the computer until the process completes;

c. Once the computer successfully reboots, no additional notifications should be received and the updates can be assumed to have completed installation; and

d. Users do not have to be actively using the computer as long as the computer is on and logged onto the network.

4. Once updates have downloaded on the workstation, users will be allotted 48 hours to save work, exit all programs and reboot (restart) the computer in order for them to take effect. If the user does not reboot the computer, it will automatically reboot after the 48-hour period has ended.

5. OCIO is to ensure the following requirements are met regarding security alerts, advisories and directives:

a. Generate internal security alerts, advisories, and directives as deemed necessary;

b. Disseminate security alerts, advisories, and directives to Chief Information Officers (CIOs), ISSPMs, Information System Security Officers (ISSOs), Network and System Administrators, or as defined by the Department or Agency;

c. Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance; and

d. Employ automated mechanisms to make security alert and advisory information available throughout FSIS as needed. This requirement is only applicable to HIGH systems.

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

A. Flaw Remediation.

1. Identify, report, and correct information systems containing software affected by recently announced software flaws and potential vulnerabilities resulting from those flaws;

2. Promptly test the effectiveness and potential side effects of newly released security relevant patches, service packs, and hot fixes on the information systems prior to installation;

3. Incorporate flaw remediation into the configuration management (CM) process;

4. Identify information systems containing software affected by recently announced software flaws, and report this information to designated official with information security responsibilities;

5. Promptly install security-relevant software updates that have been tested and approved for installation;

6. Employ automated mechanisms to periodically, and on demand, determine the state of information system components regarding flaw remediation; and

7. Centrally manage the flaw remediation process and install updates automatically. 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*.

B. **Malicious Code Protection.**

1. Employ malicious code protection mechanisms that detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, and spyware) at critical information system entry and exit points. Malicious code can be transported by:

    a. Electronic mail;

    b. Electronic mail attachments;

    c. Internet access;

    d. Removable media (e.g., USB devices, or compact disks); and

    e. Exploiting information system vulnerabilities.

2. Update malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with CM policy and procedures;

3. Configure malicious code protection mechanisms to:

    a. Perform monthly scans of the information system;

    b. Perform real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy;

    c. Block and quarantine malicious code, and send an alert to the administrator in response to malicious code detection;

    d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system;

    e. Centrally manage malicious code protection mechanisms; and

    f. Update malicious code protection mechanisms automatically.

C. **Information System Monitoring.**

1. Monitor events on information systems, detect attacks, and provide identification of unauthorized system use in accordance with Department or Agency policy and incident response processes and procedures;

2. Deploy monitoring devices within the information system to track specific types of system activity that may be of interest to the Agency;

3. Employ a wireless intrusion detection system to identify rogue wireless devices, and to detect attack attempts and potential compromises or breaches to the information system;

4. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion;

5. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to FSIS operations and assets or individuals based on law enforcement information, intelligence information, or other credible information sources;

6. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable Federal laws, Executive orders, directives, policies, and regulations;

7. Employ automated tools to support near real-time analysis of events;

8. Continuously monitor inbound and outbound communications for unusual or unauthorized activities or conditions;

9. Provide near real-time alerts to all applicable parties when indications of compromise or potential compromise occur (e.g., unusual or unauthorized activities defined by the United States Computer Emergency Readiness Team (US-CERT); and

10. Identify unauthorized use of the information system through input from audit logs, intrusion detection system and intrusion protection system.

D. **Security Functionality Verification.** The following requirements are only applicable to HIGH systems:

1. Verify the correct operation of security functions on system startup and restart and notify the system administrator when anomalies are discovered; and

2. Verify security functionality as it applies to all security functions. For those security functions that are not able to execute automated self-tests, either implement compensating security controls or explicitly accept the risk of not performing the required verification.

E. **Software, Firmware, and Information Integrity.**

1. Detect and protect against unauthorized changes to software, firmware, and information;

2. Perform an integrity check of software, firmware, and information, on information systems, that looks for evidence of information tampering, errors, and omissions.

3. Employ good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, and cryptographic hashes);

4. Reassess the integrity of software, firmware, and information by performing monthly integrity scans of the system;

5. Incorporate the detection of unauthorized security-relevant changes to the information system into the organizational incident response capability;

6. Use tools to automatically monitor the integrity of the information system and the applications being hosted;

7. For HIGH systems only:

   a. Employ automated tools that provide notification to appropriate individuals when discrepancies are discovered during integrity verification;

b. Follow the procedures identified in the system security plan (SSP) or contingency plan (CP), when integrity violations are discovered;

c. Prohibit the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and

d. Provide exceptions to the source code requirement only for compelling mission or operational requirements and with the approval of the authorizing official.

F. **Spam Protection.**

1. Employ spam protection mechanisms at information system entry and exit points and at work stations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, and other common means;

2. Automatically update spam protection mechanisms (including signature definitions) when new releases are available in accordance with CM policy and procedures; and

3. Centrally manage spam protection mechanisms.

G. **Information Input Validation.** Check the validity of information inputs and verify that inputs match specified definitions for format and content.

H. **Error Handling.**

1. Identify and handle error conditions in an expeditious manner without providing information that could be exploited by adversaries;

2. Ensure error messages are revealed only to authorized personnel;

3. Ensure error messages generated by the information system provide timely and useful information without revealing potentially harmful information that could be used by adversaries; and

4. Ensure personally identifiable information (PII) and other sensitive information (e.g., account numbers, social security numbers, and credit card numbers) is not listed in error logs or associated administrative messages.

I. **Information Handling and Retention.** Handle and retain information within the system and output from the information system in accordance with applicable laws, Executive orders, directives, policies, regulations, standards, and operational requirements.

J. **Memory Protection.** Implement data execution prevention and address space layout randomization to protect its memory from unauthorized code execution.

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 system and information integrity, 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