FSIS DIRECTIVE

1306.14 Revision 2	9/15/16

MEDIA PROTECTION

I. PURPOSE

This directive lists media protection (MP) requirements for information systems 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 1306.14, Revision 1, *Media Protection (MP)*, 12/21/12

III. BACKGROUND

A. Media are physical devices or writing surfaces on which information is recorded, stored, or printed. These can include digital media, non-digital media, portable and mobile computing, and communications devices with information storage capability.

B. MP ensures that only authorized users have access to information in digital media (e.g., magnetic tapes, external or removable hard drives, flash or thumb drives, compact disks), non-digital media (e.g., paper, microfilm), portable and mobile computing, and communications devices with information storage capability (e.g., laptop computers, smartphones, cellular telephones, telephone systems) when removed from the information system.

C. 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.

D. 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), to strengthen 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.

E. NIST SP 800-53, Revision 4, outlines the controls addressed by MP. The selection and employment of appropriate security controls for an information system are important tasks 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. **FSIS System Owners.** System owners are FSIS employees that are designated by their specific program areas and may be from program areas outside of OCIO. System owners are to:

1. Assist in the development and maintenance of detailed operating procedures to satisfy appropriate MP security controls; and

2. Ensure only authorized users have access to digital or printed media.

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 MP and this directive; and

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

V. ROLES AND RESPONSIBILITIES FOR OCIO

A. **OCIO Chief Information Officer.** Supports and promotes MP throughout the Agency.

B. **OCIO Information System Security Program Manager (ISSPM).** Ensures collaboration among organizational entities and compliance with the MP controls. In addition, the ISSPM:

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

2. Ensures Plan of Action and Milestones (POA&Ms) are developed and maintained, as needed.

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

A. **Media Access.** Restrict access to information system media to authorized individuals only. Information system media includes:

1. Both digital and non-digital media;

2. Portable and mobile computing; and

3. Communication devices with information storage capability.

B. **Media Marking.**

1. Affix external labels to removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information;

2. Perform an assessment of risk on the media requiring labeling to:

a. Determine if media exempt from labeling is within an FSIS-controlled environment. This includes removable information system media for both digital media and non-digital media; and

b. Determine that the information is publicly releasable.

3. Document the media requiring labeling and the specific measures taken to afford such protection.

C. **Media Storage.**

1. Physically control and securely store information system media within controlled areas;

2. Assess and document the risk associated with the media requiring physical protection; and

3. Protect identified information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

D. **Media Transport.**

1. Protect and control information system media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel;

2. Maintain accountability for information system media during transport outside of controlled areas;

3. Assess and document the risk and specific measures taken that are associated with the media requiring protection during transport. This assessment guides the selection and use of appropriate storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside FSIS (e.g., U.S. Postal Service or a commercial transport or delivery service);

4. Document activities associated with the transport of information system media using the approved transport carrier log;

5. Restrict the activities associated with the transport of information system media to authorized personnel; and

6. Employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

E. **Media Sanitization.**

1. Sanitize information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse. Sanitization techniques include: clearing: purging, and destroying media information and preventing the disclosure of organizational information to unauthorized individuals when such media is reused or disposed;

2. Employ sanitization mechanisms and ensure that they align with their corresponding information categories;

3. Use discretion when using sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on FSIS or individuals if released for reuse or disposal;

4. Review, approve, track, document, and verify media sanitization and disposal actions. 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*;

5. Periodically (system owners determine the frequency) test sanitization equipment and procedures to verify the intended sanitization is being achieved. This requirement is only applicable to HIGH systems; and

6. Apply nondestructive sanitization to portable, removable storage devices prior to connecting such devices to the information system when said devices have been used in any non-government system. This requirement is only applicable to HIGH systems.

F. **Media Use.**

1. Restrict the use of digital and non-digital media on information systems and components using Agency-defined safeguards; and

2. Prohibit the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

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 MP, 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.

Assistant Administrator
Office of Policy and Program Development