FSIS DIRECTIVE

1306.18	9/29/16

SAFEGUARDING MOBILE OR PORTABLE ELECTRONIC EQUIPMENT AND DATA

I. PURPOSE

A. The directive is to provide awareness to all FSIS personnel of the requirements and procedures used for safeguarding FSIS mobile or portable electronic equipment and data as stated in National Institute of Science and Technology (NIST) Special Publication (SP), 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. This includes electronic equipment and data when in an official foreign travel status. The following policy informs Government-provided mobile or portable device users of their allowable usage and features available for business and limited personal use. Mobile devices are also referred to as handheld devices or handheld computers.

B. This directive also serves to make clear the responsibility of FSIS mobile or portable device users to ensure the appropriate care of the Government-furnished equipment entrusted to them. Failure of FSIS personnel to adhere to the guidelines listed in this directive may result in personal liability or retraction of device privileges.

II. CANCELLATION

FSIS Directive 1306.17, *Safeguarding Electronic Equipment and Data During Foreign Travel*, 8/16/11

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. 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.

C. NIST SP 800-53, Revision 4, outlines the controls for safeguarding equipment and data. 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. PRIVACY EXPECTATIONS

A. Government employees do not have a right, nor should they have an expectation, of privacy while using Government-provided devices at any time, including accessing the Internet and using e-mail and

voice communications. To the extent that employees wish that their private activities remain private, they should avoid using a Government-provided device for personal use. By accepting the Government-provided device, employees imply their consent to disclosing or monitoring of their device usage, including the contents of any files or information maintained or passed through that device.

B. FSIS discourages the use of pre-installed or unauthorized apps on government-furnished mobile devices, except for MobileIron, TouchDown (for Android devices only) and all FSIS-developed and managed apps. Additional information regarding FSIS Mobile apps is available on the FSIS Website. Certain apps require the user to input personal information, which can lead to privacy breaches. This concern also extends to the use of apps on personal mobile devices. FSIS strongly encourages employees to thoroughly read all disclaimers or End User License Agreements to ensure all sign-up requirements are known before consenting. For more information on protecting your information on mobile apps, visit the Federal Trade Commission's web site on mobile device safety and privacy.

C. For additional information on apps approved for use on the Agency's government-furnished mobile devices, please contact the Office of the Chief Information Officer (OCIO) Configuration Management Team at ociocmteam@fsis.usda.gov.

V. ROLES AND RESPONSIBILITIES

A. **Office of the Chief Information Officer (OCIO) is to:**

1. Provide oversight and management of mobile or portable devices;

2. Ensure compliance with all Federal laws, regulations, and directives relating to safeguarding electronic equipment and data;

3. Ensure information security policy and standard operating procedures are developed, maintained, and distributed, and that they comply with Federal Information Processing Standards (FIPS), FISMA, NIST, Office of Management and Budget (OMB), USDA, and FSIS directives; and

4. Promote and support safeguarding electronic equipment and data throughout FSIS.

B. **OCIO Information Assurance Division (IAD) is to:**

1. Establish usage restrictions and implementation guidance, authorize connections based on usage restrictions and implementation guidance, monitor for unauthorized connections, enforce requirements for the connection, disable the functionality that will allow the execution of code, and employ cryptographic mechanisms to protect the confidentiality and integrity of mobile or portable devices;

2. Work with the OCIO Service Desk to define the necessary configuration and handling requirements for mobile or portable equipment maintained and distributed by FSIS; and

3. Ensure collaboration within FSIS on safeguarding mobile devices and data.

VI. NIST SP 800-53 REVISION 4 REQUIREMENTS

A. **Device Identification and Authentication.** OCIO ensures the information system identifies and authenticates (i.e., multifactor authentication, hardware tokens, Smart Cards) laptops, desktop computers, MiFi devices (i.e., mobile hot spots) and personal digital assistants before a connection is allowed to be established to an information system.

B. **Information and Shared IT Resources.** FSIS personnel are to prevent unauthorized and unintended information transfer via IT shared resources.

C. **Access Enforcement. OCIO is to:**

1. Enforce assigned authorizations controlling access to the system; and

2. Restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

D. **Information Flow Enforcement. OCIO is to:**

1. Enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems;

2. Implement information flow control enforcement as a basis for flow control decisions using explicit labels on information, source, and destination objects; and

3. Implement information flow control enforcement as a basis for flow control decisions using protected processing domains (e.g., domain-type enforcement) and dynamic security policy mechanics.

E. **Remote Access. OCIO is to:**

1. Document allowed methods of remote access to information systems;

2. Establish usage restrictions and implementation guidance for each allowed remote access method;

3. Monitor for unauthorized remote access to the information system;

4. Authorize remote access to the information system prior to the connection;

5. Enforce requirements for remote connections to the information system;

6. Employ automated mechanisms facilitating monitoring and control of remote access methods;

7. Use cryptography to protect confidentiality and integrity of remote access sessions;

8. Control remote access through a limited number of managed access control points;

9. Authorize the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and document the rationale for such access in the System Security Plan (SSP) for the information system;

10. Monitor for unauthorized remote connection to the information system continually with automated notification to the system administrator(s), and take appropriate action if an unauthorized connection is discovered;

11. Ensure that remote sessions for accessing security functions as defined in the SSP employ 2-Factor Authentication. All remote session activity for both regular and security related functions are to be audited; and

12. Disable Department or Agency restricted network protocols (e.g., Telnet, Rlogin, and any other Agency-defined non-secure protocols as defined in the (SSP), except for explicitly identified components in support of specific operational requirements.

F. **Continuous Monitoring.** FSIS personnel are to be aware that there is a process in place to maintain a current security status for one or more mobile or portable devices or MiFis. The process includes:

1. Developing a strategy to regularly evaluate selected controls and metrics;

2. Recording and evaluating relevant events and the effectiveness of the enterprise in dealing with those events; and

3. Recording changes to controls or changes that affect risks.

G. **Configuration Settings. OCIO is to:**

1. Establish mandatory configuration settings for mobile or portable devices employed within the organization using baselines from the NIST National Checklist Program (NCP) as modified by the Department. Where baselines are not available, contact the vendor for recommendations or use industry best practices;

2. Implement configuration settings;

3. Identify, document, and approve exceptions from the mandatory configuration settings for mobile or portable devices based on explicit operational requirements; and

4. Monitor and control changes to the configuration settings for mobile or portable devices in accordance with organizational policies and procedures.

H. **Identification and Authentication for Organizational Users (when applicable). System Owners are to:**

1. Ensure the mobile or portable devices uniquely identify and authenticate organizational users or processes acting on behalf of users, where possible (e.g., login scripts);

2. Employ the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof to authenticate user identities;

3. Ensure a personal identity verification credential is used in the unique identification and authentication of Federal employees; and

4. Employ identification and authentication mechanisms at the mobile or portable device level (e.g., at access authentication) for identifying and authenticating users when stricter controls are necessary.

I. **Protection of Information at Rest (when applicable). System owners are to:**

1. Ensure the mobile or portable devices protect the confidentiality and integrity of information at rest;

2. Employ cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures; and

3. Employ alternative mechanisms to achieve confidentiality and integrity protections, as appropriate.

J. **Flaw Remediation. OCIO is to:**

1. Identify, report, and correct mobile or portable devices 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 configuration management as an emergency change;

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; and

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

VII. DEDICATED FOREIGN TRAVEL ELECTRONIC DEVICE (DFTED)

A. **Mobile or portable device users are to:**

1. Ensure their duties are performed in accordance with user instructions in this directive and with their user agreement on file;

2. Protect their Government-issued device from theft, damage, abuse, and unauthorized use and configuration modification;

3. When scheduled for foreign travel, request equipment by submitting a FootPrints ticket or calling the Service Desk at least 5 business days in advance;

4. Ensure that unauthorized configuration modifications are not made;

5. Notify the FSIS Service Desk within one hour or as soon as possible after the device is missing or stolen. The FSIS Service desk will lock and disable the device upon notification. Immediately report the loss, theft, or compromise of any device in accordance with FSIS Directive 1300.7, *Managing Information Technology (IT) Resources*;

6. Comply with FSIS appropriate use policies when using the device;

7. Abide by the law governing the use of mobile or portable cell phones or smartphones while driving (e.g., hands-free use and/or texting);

8. Ensure the physical security of FSIS mobile or portable devices at all times. Mobile or portable devices must not place in checked baggage or left unattended when traveling; and

9. Immediately report the loss, theft, or compromise of any device while on foreign travel in accordance with FSIS Directive 1300.7.

B. Only FSIS DFTEDs (e.g., laptops, portable electronic storage devices, and smartphones) will be used to store, transmit, or process Agency information when in official foreign travel status.

C. All DFTEDs are to:

1. Have full-disk encryption; and

2. Be assigned to the FSIS DFTED pool.

D. DFTEDs are not to be connected (physically nor by tethering) to the FSIS network upon return from foreign travel.

E. DFTEDs are to be returned to the Service Desk within 10 business days upon return from foreign travel.

F. Two-factor authentication is required for all remote access. Travelers are required to have a LincPass and know their PIN. Smartphones do not use two-factor authentication and are exempt from this requirement.

G. DFTEDs are prohibited from using removable memory cards.

H. **The OCIO service desk is to:**

1. Manage IT related issues from creation to resolution through the use of an Automatic Call Distribution (ACD) system with interactive menus, intelligent routing, and integrated voicemail. The ACD system will operate 24 hour a day, 7 days a week to field service requests using a centralized incident system of record. Service requests can be fielded via call processing or user-submitted emails and incidents;

2. Work with the IAD to define the necessary configuration and handling requirements for mobile or portable devices maintained and distributed by FSIS;

3. Ensure collaboration within FSIS on safeguarding electronic equipment and data during foreign travel; and

4. Inventory and issue mobile or portable devices and data.

I. **Mobile or portable device owners are to:**

1. Ensure appropriate procedures are in place to meet data safeguarding requirements; and

2. Ensure mobile or portable devices meet the security requirements for use of application and data to mobile or portable devices before authorization is granted.

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 safeguarding mobile or portable electronic equipment and data, 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.

C. The FSIS Service Desk can be reached at 1-800-473-9135, 24 hours a day.

Assistant Administrator
Office of Policy and Program Development