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

# FSIS DIRECTIVE	1306.17	8/16/11

SAFEGUARDING ELECTRONIC EQUIPMENT AND DATA DURING FOREIGN TRAVEL

I. PURPOSE

This directive establishes mandatory requirements and assigns roles and responsibilities for safeguarding Agency electronic equipment and data when in an official foreign travel status.

II. (RESERVED)

III. (RESERVED)

IV. REFERENCES

DR 3505-002, Wireless Networking Security Policy
Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, Security Requirements for Cryptographic Modules
FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
FSIS Directive 1300.7, Managing Information Technology (IT) Resources
FSIS Directive 4735.3, Employee Responsibilities and Conduct
Homeland Security Presidential Directive 12 (HSPD-12)
National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook
NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations
Office of Management and Budget (OMB) Memorandum M-06-16, Protection of Sensitive Agency Information
OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
Public Law 107-347, Title III, E-Government Act of 2002

V. ABBREVIATIONS

The following appear in their shortened form in this directive:

DFTED	Dedicated Foreign Travel Electronic Device
FISMA	Federal Information Security Management Act
ISSP	Information System Security Program
ISSPM	Information System Security Program Manager
IT	Information Technology
NIST SP	National Institute of Standards and Technology Special Publication
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget

VI. POLICY

It is FSIS policy to ensure 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 and USDA regulations.

VII. DEFINITIONS

A. **Authentication**. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

B. **Information System**. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, storage, or disposition of information. An information system must have logical boundaries around a set of processes, communications, and storage, and the boundaries must:

1. Be under the same direct management control.

2. Have the same function or mission objective.

3. Have essentially the same operational and security needs.

4. Reside in the same general operating environment.

C. **IT**. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

D. **System Owner**. A person or organization having responsibility for the development, procurement, integration, modification, operation and maintenance, and final disposition of an information system.

E. **System User**. An individual authorized to utilize FSIS IT resources.

VIII. BACKGROUND

A. FISMA was passed by Congress and signed into law by the President as Public Law 107-347, Title III, E-Government Act of 2002. 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, NIST, and 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.

B. NIST SP 800-53, Revision 3, outlines the controls to be addressed for safeguarding 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. Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

IX. DFTED REQUIREMENTS

A. Only FSIS DFTEDs (**examples**: laptops, portable electronic storage devices, and Blackberry™ devices) will be used to store, transmit, or process Agency information when in official foreign travel status.

B. All DFTEDs must:

1. Have full-disk encryption.

2. Be assigned to the FSIS DFTED pool.

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

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

E. Two-factor authentication is required for all remote access. Travelers are required to have a LincPass and know their PIN. (**NOTE**: Blackberry™ devices do not use two-factor authentication and are exempt from this requirement.)

F. DFTEDs are prohibited from using removable memory cards.

.

X. ROLES AND RESPONSIBILITIES

A. **OCIO**.

1. Ensures compliance with all Federal laws, regulations, and directives relating to safeguarding data.

2. Ensures information security policy and standard operating procedures are developed, maintained, and distributed, and that they comply with FISMA, NIST, OMB, USDA, and FSIS directives.

3. Promotes and supports safeguarding electronic equipment and data throughout the Agency.

B. **ISSP**.

1. Works with the Service Desk to define the necessary configuration and handling requirements for equipment maintained and distributed as part of the DFTED pool.

2. Ensures collaboration within FSIS on safeguarding data during foreign travel.

C. **System Owners**.

1. Ensure appropriate procedures are in place to meet DFTED requirements.

2. Ensure DFTEDs meet the security requirements before authorization is granted for use on foreign travel.

D. **System Users**.

1. Ensure their duties are performed in accordance with this policy.

2. Request equipment by submitting a FootPrints ticket or calling the Service Desk at least 5 business days in advance of foreign travel.

3. Ensure the physical security of FSIS laptops, portable electronic storage devices, or Blackberry™ devices at all times and must not:

   a. Place in checked baggage when traveling.

   b. Leave unattended.

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

XI. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

FSIS Directive 1300.7 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 outlines the disciplinary action that FSIS may take when policies are violated.

XII. ADDITIONAL INFORMATION

A. USDA departmental directives are located at http://www.ocio.usda.gov/. FSIS directives and notices are located on *InsideFSIS* at http://inside.fsis.usda.gov/.

B. For additional information about this directive, contact the FSIS Information System Security Program at FSIS_Information_Security@fsis.usda.gov.

C. For additional information about LincPass (USDA's HSPD-12 compliant ID card), visit http://hspd12.usda.gov/.

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

for Assistant Administrator
Office of Management