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

# FSIS DIRECTIVE

1306.22 | 7/3/17

## INTERNATIONAL AND DOMESTIC USE OF FSIS GOVERNMENT-FURNISHED EQUIPMENT

### I. PURPOSE

This directive provides FSIS Federal and non-Federal employees (e.g., contractors) with instructions regarding the acceptable and unacceptable use of FSIS government-furnished equipment (GFE) (e.g., telecommunications resources, computers, laptops, and smartphones) and Government-issued e-mail addresses when conducting government business both domestically and internationally. This directive also states the need for some employees to complete an FSIS mobile device agreement.

### II. BACKGROUND

A. DR 3300-001 explains that USDA employees are allowed the limited personal use of telecommunications resources (e.g., telephones, facsimile, electronic messaging, computer equipment, and the Internet) in the workplace on an occasional basis, provided that the use involves minimal expense to the Government and does not interfere with official business. Official Government business takes precedence over the personal use of telecommunications resources. Agencies and staff offices may supplement DR 3300-001 as required to clarify internal operating procedures.

B. FSIS Directive 1300.7, *Managing Information Technology (IT) Resources*, sets out the Agency's policy regarding the use of GFE. This directive restricts the use of FSIS e-mail addresses (e.g., John.Public@fsis.usda.gov) to only Government-related business. Employees are not to use their FSIS email address for any other purpose, such as online shopping, setting other e-mail accounts (e.g., Yahoo, Google), or subscriptions to non-government publications. The use of government e-mail addresses in these ways poses an increased risk to Agency, Departmental, and Federal infrastructure, data, and resources.

C. Employees are to be aware that the FSIS Office of Chief Information Officer (OCIO) routinely monitors and controls all computer access points (e.g., Universal Serial Bus, FireWire®, infrared, Bluetooth, wireless Ethernet). There is no right to privacy on U.S. Government systems, e-mail, or equipment.

### III. FSIS EMPLOYEE RESPONSIBILITIES

A. Employees are to complete annual Federal and USDA mandated training (e.g., Security Awareness and Privacy training).

B. Employees are to use the USDA-FSIS Local Area Network (LAN) or Virtual Private Network (VPN) for Internet browsing using GFE, including limited use during the employee's personal time (e.g., weekends if the employee has access to the work site or to GFE at home, before and after work, lunchtime, or during scheduled break periods). No off-Agency network Internet access, except when necessary to connect to the USDA/FSIS network, is permitted.

C. Employees are not to access the USDA-FSIS network or process FSIS sensitive-but-unclassified information on any computer or device that is not FSIS GFE.

D. Employees are to ensure that all removable media devices, such as CDs, DVDs, removable hard drives, and thumb drives containing sensitive but unclassified information, including personally identifiable information (PII), are OCIO-approved devices which are encrypted at the Federal Information Processing Standards (FIPS)140-2 standard.

E. Employees are to abide by traffic laws governing the use of mobile phones or portable devices while driving (e.g., some states require drivers to remain hands free, no texting).

F. While on personal leave and traveling internationally, FSIS will not permit GFE issuance. An approved official travel authorization in Concur® is required prior to OCIO issuing GFE for use on official international travel. FSIS employees are to adhere to the FSIS GFE rules for international travel to include the following:

1. Pre-Travel:

    a. Obtain travel authorization in Concur®;

    b. Request Dedicated Foreign Travel Electronic Device (DFTED) equipment from OCIO by submitting a FootPrints service ticket or call the FSIS Service Desk at least five (5) business days in advance of travel; and

    c. Obtain approved GFE for international business travel, to include: laptops, portable electronic storage devices, and smartphones, hereafter, referred to DFTEDs. Travelers are not to use their standard domestic-issued GFE.

2. During Travel:

    a. Disable Wi-Fi when the DFTED is not in use;

    b. Protect DFTEDs from theft, damage, abuse, and unauthorized use and configuration modification;

    c. Ensure that only DFTEDs are used to store, transmit, or process FSIS information when on approved international travel;

    d. Ensure the physical security of the DFTEDs at all times. DFTEDs must not be placed in a checked baggage or left unattended when traveling;

    e. Notify the FSIS Service Desk within one (1) hour or as soon as possible after any DFTED is missing or stolen. The FSIS Service Desk will lock and disable the DFTED upon notification; and

    f. Immediately report the loss, theft or compromise of the DFTED in accordance with FSIS Directive 1300.7.

3. Post-Travel:

    a. Ensure DFTEDs are NOT connected physically (e.g., LAN) nor by tethering (e.g., VPN) to the FSIS network upon return from international travel;

    b. Ensure DFTEDs are returned to the FSIS Service Desk within ten (10) business days upon return from international travel;

    c. The FSIS Service Desk is to bring the DFTEDs to the FSIS Security Operations Center (SOC) for post travel inspection; and

    d. The FSIS Service Desk is to wipe or reimage the DFTEDs before returning them to the loaner pool.

G. Employees are to lock up and secure DFTEDs to the best of their ability when not in use or when in storage.

## IV. PROHIBITED USES OF GFE

FSIS explicitly prohibits the use of GFE (including government-issued e-mail addresses) for:

1. Accessing or processing pornographic material, gaming or gambling content;

2. Accessing non-work-related streaming internet radio or media;

3. Giving out personal information about another person outside of work, including home addresses and phone numbers, unless the employee's supervisor has approved providing this information for emergency purposes;

4. Installing software (including shareware, freeware and toolbars);

**NOTE**: Only an FSIS Service Desk technician or authorized Office of Chief Information Office information technology (OCIO IT) specialist may install Technical Change Control Board-approved hardware and software to Agency computers, unless otherwise directed by OCIO.

5. Accessing file-sharing services (e.g., Dropbox, Google Drive, One Drive);

6. Sharing FSIS network accounts. Accounts are not to be shared and are to be used solely on USDA network systems for authorized business purposes;

7. Connecting non-FSIS computers to the FSIS network, either directly or through a Virtual Private Network (VPN) connection, except for authorized use of approved Secure Socket Layer (SSL) VPN by OCIO;

8. Using the network for commercial or for-profit purposes;

9. Seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users;

10. Misrepresenting other users on the network;

11. Using the network to disrupt the use of the network by others;

12. Abusing, destroying, or modifying hardware or software in any way;

13. Using the network to develop programs that harass other users or infiltrate a computer or computing system or damage the software components of a computer or computing system;

14. Sending hate mail, chain letters, harassment, discriminatory remarks or content, or other inappropriate behaviors;

15. Downloading, copying, otherwise duplicating, or distributing copyrighted materials without the specific written permission of the copyright owner;

16. Using the network for any unlawful purpose;

17. Using profanity, obscenity, racist terms, or other language or content that may be offensive to another user;

18. Leaving FSIS computers in an operational state (leaving unlocked) while unattended; and

19. Using any untrusted networks, such as those in Internet Cafes and Coffee Shops offering, "Free Public Wi-Fi."

## V. FSIS MOBILE DEVICE AGREEMENT

FSIS employees and contract employees who use mobile devices (e.g., smart phones and tablets) provided by FSIS for work purposes are to review the rules of behavior and sign the FSIS Mobile Acceptable Use and Rules of Behavior Agreement (Level 2 eAuthentication is required to access this information and form on InsideFSIS). After completing the agreement, employees are to submit it to their supervisor. Supervisors are to maintain signed copies of the agreements for all of their employees that use mobile devices.

## VI. QUESTIONS

Refer questions regarding this notice to the FSIS Security Operations Center at: OCIOSecurityOperationsCenter@fsis.usda.gov.

Assistant Administrator
Office of Policy and Program Development