United States Department of Agriculture

Food Safety and Inspection Service

FSIS Directive 1300.7

Revision 1

Managing Information Technology (IT) Resources

MANAGING INFORMATION TECHNOLOGY (IT) RESOURCES

TABLE OF CONTENTS

PART ONE—BASIC PROVISIONS

PART TWO—PORTABLE ELECTRONIC DEVICES

PART THREE—COMPUTER EQUIPMENT USE

PART FOUR—COMPUTER CONFIGURATION STANDARDS

PART FIVE—INTERNET USE

PART SIX—E-MAIL GUIDANCE

PART SEVEN—REIMBURSEMENT POLICY FOR BROADBAND SERVICES

PART EIGHT—FSIS WIRELESS SERVICE ACQUISITIONS

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

FSIS DIRECTIVE

1300.7
REVISION 1

6/3/09

MANAGING INFORMATION TECHNOLOGY (IT) RESOURCES

PART ONE—BASIC PROVISIONS

I. PURPOSE

This directive:

A. Describes FSIS IT policy.

B. Establishes procedures and responsibilities for using FSIS IT Resources to:

1. Protect the employee and FSIS.

2. Ensure the most appropriate and efficient allocation of resources.

3. Minimize the risk to FSIS from inappropriate use via:

a. Virus attacks.

b. Compromised network systems and services.

C. Updates Office of Chief Information Officer's (OCIO's) policy for reimbursement of IT services.

II. CANCELLATION

This directive cancels:

A. FSIS Directive 1300.1, Revision 3, Amendment 1, FSIS Information Resources Management, dated 6/19/96.

B. FSIS Directive 1300.7, Managing Information Technology Resources, dated 12/10/07.

DISTRIBUTION:
All Employees

OPI:
OPEER – Information Technology Policy and Capitol Planning Division

C. FSIS Notice 14-09, FSIS Wireless Service Acquisitions, dated 2/24/09.

D. FSIS Notice 106-08, Reimbursement Policy for Broadband Services, dated 12/31/08.

E. FSIS Notice 84-08, Funding for Blackberry™ Devices, dated 11/18/08.

III. REASON FOR REISSUANCE

This directive is being reissued to:

A. Combine the following IT policies into a central location:

1. FSIS Notice 14-09, FSIS Wireless Service Acquisitions, dated 2/24/09.

2. FSIS Notice 106-08, Reimbursement Policy for Broadband Services, dated 12/31/08.

3. FSIS Notice 84-08, Funding for Blackberry™ Devices, dated 11/18/08.

B. Establish FSIS wireless service acquisitions policy and procedures for the purchase of IT equipment.

C. Change the name of the Enterprise Change Control Board to Technical Change Control Board (TCCB).

D. Establish that Instant Messaging (IM) is prohibited on Government-owned equipment (GOE) for communication external to FSIS.

IV. REFERENCES

Directive 1310.3, Technical Change Control Board (TCCB)
Directive 1320.2, Systems Development Life Cycle

DM-3525-002, USDA Internet Use and Copyright Restrictions
DR 3080-001, Records Management
DR 3300-001, Telecommunications & Internet Services and Use
5 CFR Part 2635.101, The Standards of Ethical Conduct
FIPS 140-2, Security Requirements for Cryptographic Modules

SF-1164, Claim for Reimbursement for Expenditures on Official Business
AD-700, Procurement Request

Web site:

https://inside.fsis.usda.gov/fsis/emp/static/global/offices/oSpace/ocioOffice/itConnection/itConnection.jsp

V. ABBREVIATIONS

The following appear in their shortened form in this directive:

CD	Compact Disk
CD-ROM	Compact Disk—Read Only Memory
CIO	Chief Information Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
DO	District Office
DR	Departmental Regulation
DSL	Digital Subscriber Line
DVD	Digital Video Disk
E-mail	Electronic Mail
EMC	Emergency Management Committee
EOE	Employee-Owned Equipment
EVDO	Evolution-Data Optimized
FIPS	Federal Information Processing Standard
GOE	Government-Owned Equipment
ID	Identification
IM	Instant Messaging
IT	Information Technology
OCIO	Office of Chief Information Officer
OFO	Office of Field Operations
OM	Office of Management
OPACE	Office of Public Affairs and Consumer Education
OPEER	Office of Program Evaluation Enforcement and Review
PC	Personal Computer
PDA	Personal Digital Assistant
PII	Personally Identifiable Identification
RFC	Request for Change
RMS	Resource Management Specialist
SES	Senior Executive Service
SSL	Secure Socket Layer
TB	Telecommunications Branch
TCCB	Technical Change Control Board
USB	Universal Serial Bus
VPN	Virtual Private Network

VI. POLICY

It is FSIS policy to provide employees with the necessary IT resources to carry out the Agency's mission. Employees and their agents are accountable for all actions performed with their user ID and password. Sharing this unique user information is prohibited. The expectation of privacy or confidentiality does not apply in your use of FSIS IT resources.

A. IT resources are used to:

1. Enhance delivery of services to the public and industry.

2. Protect Agency data and secure the overall infrastructure.

B. Employees must take all necessary steps to protect FSIS IT resources and media (**examples**: hard disks, floppy disks, CD-ROMs and tapes, removable drives and media, and DVDs).

C. Employees should immediately call the FSIS Service Desk at 202–720–4016 (headquarter employees), or 800–473–9135 (field employees), to report any unusual or unexplainable changes to IT resources such as:

1. Vanishing files.

2. Slow or disrupted network service.

3. Pop-up windows.

D. GOE should only be kept in vehicles when traveling to perform official business or travel to and from the workplace. GOE and media must:

1. Never be left in plain view within the vehicle.

2. Always be locked in the vehicle and out of view.

3. Be secure at all times when not stored at the worksite.

E. GOE and media must not be placed in checked baggage when traveling. GOE must always be kept in sight.

F. Personal and privacy data should not be stored on mobile GOE (**examples**: laptop, Blackberry™, or thumb drive) or media unless the data are encrypted and approved for use.

G. Immediately report any loss or theft of IT resources in the following order:

1. USDA at 888–926–2373, 24 hours a day.

2. FSIS Service Desk at 202–720–4016, from 7:30 a.m. to 4:30 p.m. eastern standard time, or 800–473–9135, from 5:00 a.m. to 11:00 p.m. central standard time. After hours, record your message and a service desk or IT specialist will respond by the next business day.

H. Immediately report PII incidents by contacting USDA at 877–744–2968 or 888–926–2373, 24 hours a day.

VII. DEFINITIONS

See Attachment 8-1 for a listing of definitions used in this directive.

VIII. APPLICABILITY

This directive applies to all FSIS employees, other Federal agencies, State and local governments, and authorized private organizations or individuals who use FSIS IT resources.

PART TWO—PORTABLE ELECTRONIC DEVICES

I. PROVISIONS

FSIS provides portable electronic devices (**example**: Blackberry™ devices) to eligible employees to access FSIS information systems for routine operations and emergency response. These devices provide:

A. Back-up communications when network disruptions occur.

B. Enhanced responsiveness and remote accessibility to managers and staff.

C. Effective communication for emergency responders.

D. Automated information access when no other access is available.

E. Off-hour project monitoring support.

F. Out-of-the-office staff access.

II. RESPONSIBILITIES

A. OCIO maintains all portable electronic device procurement fees and monthly service fees for:

1. SES.

2. EMC (maximum of three employees per program area).

3. Headquarters-level COOP and Crisis Action Team personnel.

4. Recall management staff.

5. OPACE recall leads (up to three employees).

6. Designated OCIO personnel.

B. Program areas are responsible for funding Blackberry™ devices and services for the following employees:

1. Program-level COOP personnel.

2. All other roles and staff.

C. OCIO must review and approve all program area portable electronic device procurement requests prior to purchasing.

D. Employees must perform duties following The Standards of Ethical Conduct (5 CFR Part 2635.101(b)(5)).

E. OCIO manages telecommunications following DR 3300-001 and other related laws and regulations. (**NOTE**: Program areas are responsible for managing their wireless accounts and submitting an annual inventory report to the OCIO.)

F. Supervisors must ensure appropriate IT use within their organizations and should be proactive in speaking with employees about authorized use, and employees should talk with their supervisors about authorized IT use.

G. Portable electronic device use is a privilege. Supervisors or other appropriate Agency officials may revoke or limit this privilege at any time.

III. ACQUISITION JUSTIFICATION

Supervisors must ensure that portable electronic devices procured, support the employee's responsibilities, related productivity, and responsiveness requirements.

IV. POLICY AND PROCEDURES ENFORCEMENT

OCIO approves new or replacement portable electronic device acquisitions and related service contracts for the program area staff. (**NOTE**: Program areas cannot procure devices that do not conform to the FSIS standard unless an exception is granted by OCIO.) Program areas must document exception requests and include supporting documentation.

A. **Acquisition Procedures**. Program areas must:

1. Comply with policy and approval requirements when ordering a device or replacing an existing device.

2. Follow the procurement ordering process after receiving approval(s).

3. Review and promptly execute payment for monthly charges.

4. Provide immediate access to the portable electronic device (for inspection, troubleshooting, forensic examination, etc.), including any passwords, upon OCIO's written request.

B. **Inventory and Property Management**.

1. OCIO monitors portable electronic device usage.

2. Program areas:

a. Ensure that staff members create a property record for all devices; recording the manufacturer, model number, serial number, assigned user, and telephone numbers.

b. Ensure that employees make equipment available for inventory.

c. Notify OCIO of user or equipment changes.

d. Provide an annual electronic inventory report to OCIO.

C. **Standard Configuration**.

1. A portable electronic device is assigned to the position, not the person, and accounted for using inventory control. Return portable electronic devices to the accountable property officer when departing from your assigned position. ■

2. A portable electronic device permits access to official e-mail and document attachments. Portable electronic devices are configured to work only with Government-owned computers.

D. **Device Replacement**. For replacement due to damage or malfunction, contact OCIO, FSIS Service Desk at 202–720–4016 (headquarter employees) or 800–473–9135 (field employees). If the device is lost or stolen, follow the instructions from Part One, subparagraphs VI. G. and H. OCIO will cancel the device from ■
accessing FSIS networks and the device will be remotely erased of all content. ■

E. **Blackberry™ Device Password Policy**. ■

1. Passwords must be five or more characters in length. Passwords ■
with five characters must contain at least one letter and one number character. ■

2. Passwords with six or more characters are not required to contain ■
a letter character. ■

3. Passwords expire after 90 days. ■

4. Ten consecutive failed login attempts will automatically and ■
entirely erase the information on the Blackberry™ device. ■

PART THREE—COMPUTER EQUIPMENT USE

OCIO funds IT equipment for the Agency by providing authorized employees with one computer loaded with the standard image. (**NOTE:** As desktop computers are replaced with laptop computers, the laptop computer will become the employee's sole computer.) Authorized field employees will be issued a semi-rugged laptop loaded with the standard image. Employees who transfer to other positions within FSIS will take their assigned computer with them.

I. ACCEPTABLE USE

A. **Personal**. Employees may have limited personal use of Government office equipment during personal time, at no additional security or privacy risk to the Government. Such limited personal use is considered an authorized use of Government property (DR 3300-001). However, supervisors or other appropriate Agency officials may further restrict personal use based on office needs or inappropriate use in the office. Limited personal use involves:

1. Minimal additional expense to the Government (**examples**: normal wear and tear, low electricity, ink, toner, or paper use).

2. Use during the employee's personal time (**examples**: weekends (if the employee has access to the work site), before and after work, lunchtime, or during scheduled break periods).

3. No interference with the Agency mission or operations.

4. FSIS standard software loaded games used during personal time as a learning tool to navigate the mouse, touchpad, or other input device.

B. **General**. Use of GOE that promotes general Agency-supported information sharing among employees is considered authorized use. In addition, employees may use GOE to communicate with recognized employee organizations. However, supervisors or other appropriate Agency officials may further restrict general use based on office needs or inappropriate use in the office. Acceptable general use involves:

1. E-mailing announcements or fliers for recognition and award events where regulations permit the use of Government funds for the function.

2. E-mailing announcements or fliers for FSIS employees leaving the Agency or retiring.

II. UNACCEPTABLE USE

Inappropriate use of GOE is prohibited. Inappropriate use includes:

A. Generating more than minimal additional expense to the Government.

B. Causing congestion, delay, or disrupted service to any Government system or equipment. **EXAMPLES**:

1. Forwarding "chain" e-mails.

2. E-mailing greeting cards.

3. Using sites that require large broadband connections, such as large-size audio or video files not needed for work purposes.

4. Downloading video, sound, pictures, or other large (greater than 500 kilobytes) file attachments.

C. Illegal or offensive activities. **EXAMPLES**:

1. Pornography.

2. Hate speech.

3. Material that ridicules a person's race, creed, religion, color, sex, disability, national origin, or sexual orientation.

4. Unauthorized acquisition, use, reproduction, transmission, or distribution of any copyrighted material including software, music, videos, etc.

D. FSIS standard software loaded games used during working hours.

E. Using GOE for commercial or "for-profit" activities such as outside employment or personal business activity. **EXAMPLES**:

1. Consulting for pay.

2. Sales.

3. Business administration transactions, such as sale of goods or services.

4. Gambling.

F. Involvement in any outside activities. **EXAMPLES**:

1. Fund-raising.

2. Endorsing products or services.

3. Participating in lobbying events.

4. Engaging in prohibited partisan political events. (**EXCEPTION**: The prohibition against engaging in political activity does not apply to Presidential appointees who have received Senate confirmation.)

III. GUIDELINES

A. Employees must not leave FSIS computers in an operational state while unattended. When leaving your computer system, manually lock the computer.

B. Files created or stored on a PC or a flash drive (personal or Government-owned) must be scanned often for virus protection prior to downloading files to a Government computer. Only approved external drives with hardware encryption or FIPS 140-2 compliant can access the government-owned computer.

C. All removable media devices, such as CDs, DVDs, removable hard drives, and thumb drives containing sensitive but unclassified information, including PII, are required to be encrypted at the FIPS 140-2 standard. Sensitive information stored on mobile devices other than laptops (**examples**: PDAs or Blackberry™ devices) will employ encryption whenever available. All mobile devices must be password protected.

D. Employees must not share their user ID or password with others.

E. EOE laptops and desktops cannot be connected to the FSIS network, either directly or through a VPN connection except for authorized use of SSL VPN by OCIO.

F. EOE portable electronic devices or PDAs cannot be connected to FSIS computers or networks.

G. Only GOE can be used to access the FSIS network or process FSIS sensitive-but-unclassified information.

H. All computer access points (serial, USB, FireWire®, infrared, Bluetooth, wireless Ethernet, etc.) are routinely monitored and controlled.

I. Limited storage of personal files on the computer is permitted. (**EXAMPLE**: An employee, during personal time, writes a letter to an insurance company, or updates their résumé.)

J. Personal files, including audio or video files, cannot be stored on FSIS network servers.

K. Audio or video files found on a local hard drive can be deleted without prior notice.

L. Employees must not download file-sharing software (**examples**: music, video file sharing, such as iTunes, Bit Torrent, IM, Napster, etc.), peer-to-peer software or games on GOE or FSIS network servers.

M. Unauthorized acquisition, use, reproduction, transmission, or distribution of any copyrighted material, including software, is strictly prohibited.

N. Employees must not install any software on GOE. Only an FSIS service desk or authorized IT specialist may install hardware and software to Agency computers, unless otherwise directed by OCIO.

O. Personal files, including photos and videos, are not to be used as screensavers or backgrounds on GOE.

P. Screensavers are not to be downloaded from the Internet. The FSIS standard image configured screensaver includes parameters for locking the computer after a prescribed time interval as a security feature and is not to be changed.

Q. All employees must complete all Federal and USDA mandated training (**example**: Security Awareness and Privacy training prior to receiving access to Agency IT resources).

IV. PASSWORD CONFIGURATION

A. Passwords must:

1. Be a minimum of 12 characters in length.

2. Not contain any dictionary words. (**NOTE**: Names that appear in a dictionary such as Jill, John, or Bill cannot be used.)

3. Contain at least one capital and one lowercase letter, one number, and a non-letter character (**examples**: % and #).

4. Not be identical to the last 24 passwords.

B. Change passwords every **60** days.

V. FILE RETENTION

A. Employees are responsible for backing up all data files.

B. Save data files, (correspondence, spreadsheets, database files, etc.) to “My Documents” either to your local hard drive or to the FSIS network server.

C. Data files saved on the local hard drive or the FSIS network server, should be backed up to a diskette, flashdrive, or CD.

VI. ACQUISITION PROCEDURES

A. Program areas must obtain OCIO review and approval before:

1. Purchasing IT equipment.

2. Purchasing or entering into IT requirements gathering or development contracts with vendors without OCIO approval.

B. Hardware on the OCIO approved list does not require an RFC. To view the current software and hardware list and documentation on the RFC process, visit the IT Connection page in *InsideFSIS* at https://inside.fsis.usda.gov/fsis/emp/static/global/offices/oSpace/ocioOffice/itConnection/itConnection.jsp.

C. To order IT hardware, the program area requisitioner should:

1. Log on to the FSIS network, open Internet Explorer, and go to http://service/footprints. Footprints is the single entry point for all IT procurements.

2. Enter IT hardware request information into Footprints, regardless of cost, by selecting “Purchase Hardware” from the approved pick list and submit request. When IT hardware items are not on the approved list, the request is routed automatically to the CM team for further processing and presentation to the TCCB. (**NOTE**: Only program area requisitioners with purchasing ability will be able to see the “ORDER PROJECT” within Footprints.)

PART FOUR—COMPUTER CONFIGURATION STANDARDS

I. STANDARDS

A. All Agency computers are loaded using the standard image for the specific computer model. Software not included in the standard image is considered supplemental and is not supported by FSIS. View the standard image list at (https://inside.fsis.usda.gov/fsis/emp/static/global/offices/oSpace/ocioOffice/itConnection/itConnection.jsp). Users must be authenticated through eAuthentication to access the list.

B. Only hardware and software approved by OCIO through the RFC process can be installed on Agency computers. This includes downloading trial software, commercial software, freeware, or upgrades from the Internet.

C. Only purchased and licensed software is installed on GOE. The software must be authorized and cannot conflict with the standard image. Loading software that deviates from the standard image is prohibited.

D. OCIO maintains FSIS purchased software and licensing documentation.

E. The minimum software for the desktop is Windows XP and Office XP.

F. The minimum software for the server operating system is Windows 2000.

G. The FSIS Service Desk does not support computers running any operating system other than Windows XP.

H. Software for personal use, Web browser plug-ins, and downloads from the Internet are not allowed unless reviewed and approved by TCCB.

I. Employees must use care when obtaining data from non-Agency sources. Occasionally, data could be packaged with embedded software. Such software can cause system problems. Contact the FSIS Service Desk at 202–720–4016 (headquarter employees) or 800–473–9135 (field employees) before accepting non-Agency software.

J. Employee-owned software is prohibited on GOE.

K. Employees must not install software or applications without approval from OCIO.

L. Employees must not alter or tamper with the system or security configuration of FSIS computer systems.

II. STANDARD IMAGE

A. OCIO establishes the standard software image after reviewing the Agency's computing needs and the Federal and departmental requirements. The standard image contains the base software to meet user computing needs, and provides uniform usage and support.

B. The standard image selection focuses on:

1. Individual software package quality.

2. Functions where a package excels or falls behind its competitors, or special and common user needs.

3. Complementary features and conversion ease among packages.

4. Retraining costs.

5. Future computer technology trends.

III. OPERATING PROCEDURES

A. OCIO maintains the following operations:

1. **Destruction of Outdated Software**. OCIO destroys outdated software and licenses. OCIO also erases installation disks and recycles the documentation.

2. **Evaluation Software**. Downloads for evaluations or software test copies from the Internet are not permitted without OCIO consent. FSIS service desk or authorized IT specialists may download an evaluation copy to a user's computer only if:

a. There is an evaluation period expiration date.

b. OCIO has approved the installation of the software.

3. **Migrating Unauthorized Software**. In the migration of a Government computer, an FSIS service desk or authorized IT specialist assists the user in submitting an RFC for seeking authorization of the unsupported software package. The migration will take place without the unsupported software package if approval is not reached within 30 days.

4. **Recycling Replaced Software**. Software is not redistributed by program areas if replaced by newer packages. Such software is "recycled" within the OCIO library system. (**NOTE**: The Agency's OCIO library system is a centralized location that houses the collection of media procured for GOE. The FSIS Service Desk maintains the library.)

a. A recycled software evaluation for requesters is based on the use and system requirements. Licensing remains centrally located and the documentation (manuals) is moved to the new user.

b. Upgraded software versions that require the original software for installation are maintained with the original software and license.

B. FSIS service desk or authorized IT specialists perform new upgrade installations to maximize installation standardization, and minimize potential problems and hazards.

IV. NEW SOFTWARE

A. OCIO funds new Enterprise-level software packages only.

B. OCIO does not fund supplemental software.

C. To order software, see Part Three, subparagraph VI. C. 1-2.

D. TCCB evaluates new software requests based on documented business needs, system requirements, compatibility with the standard image, and compliance with Federal and Departmental policies. Based on the evaluation, the TCCB:

1. Recommends an alternate software package.

2. Advises the user that the requested software is approved for purchasing.

E. When approved, the user orders the software following the appropriate procurement process.

F. An FSIS service desk or authorized IT specialist loads the supplemental software.

1. If a problem occurs with the supplemental software that affects the standard image, the specialist will reload the standard image to fix the problem.

2. OCIO maintains original installation diskettes or software and licensing documentation for security and legal reasons. The FSIS service desk or authorized IT specialist keeps copies of rescue diskettes and other software, and where possible, the user maintains software documentation (manuals) for training purposes.

V. RELOADING SUPPLEMENTAL SOFTWARE

A. When GOE fails and the user maintains supplemental software, the FSIS service desk or authorized IT specialist can reload the operating system if the software ■

1. **More Than 3 Years Old and The Software Is Available**. The FSIS ■ service desk or authorized IT specialist reloads the software and informs the user to purchase the most recent version of the software within 30 days.

2. **Less Than 3 Years Old and The Software Is Available**. The FSIS ■ service desk or authorized IT specialist reloads the software and stores the media in the central repository within OCIO.

B. If the user or the FSIS Service Desk does not have the software, the ■ application is not reloaded. The FSIS service desk or authorized IT specialist assists the user in reordering the software. The FSIS service desk or authorized IT specialist loads the software when it arrives and maintains the media in the central repository within OCIO.

PART FIVE—INTERNET USE

I. BACKGROUND

The Internet provides FSIS employees the opportunity to locate and use current and historical data from multiple sources worldwide in their decision-making processes. These networks subscribe to a common set of standards and protocols. Users have worldwide access to Internet hosts and their associated applications and databases. Employees are expected to use the Internet to improve their job knowledge or access scientific, technical, and other information relevant to the Agency's mission.

II. RESPONSIBILITY

A. **User Responsibility**. GOE is for official use and authorized purposes. Use serves as consent to security monitoring of any type. This includes incidental and personal uses, whether authorized or unauthorized. The expectation of privacy or confidentiality does not apply in your use of FSIS access to the Internet.

1. Employees are expected to communicate electronically in a manner that reflects positively on themselves and on the Agency.

2. Employees who accidentally access an unacceptable Web site must not open the site. Click out of the site and immediately close the browser.

3. Employees must not engage in any unlawful activity.

4. Employees must not imply that they are acting in an official capacity when using GOE for non-Government purposes.

5. Employees must not engage in any activity that would compromise the security of any Government host computer or FSIS network.

6. Employees must not disclose or share log-in passwords with others.

7. Employees must not download file-sharing software (**examples**: music, video file sharing software such as iTunes, Bit Torrant, IM, Napster, etc.), peer-to-peer software, games, or copyrighted material on GOE or FSIS networks.

B. **Supervisory Responsibility**. Supervisors have final authority in determining whether an employee requires Internet access to accomplish assigned duties. The supervisor will:

1. Authorize Internet access to FSIS employees in order to conduct the official business of the Agency.

2 Provide guidance on proper Internet use according to this directive.

3. Advise employees of the restriction against personal use of Agency Internet access resources from other than departmental or partner facilities.

4. Determine the appropriateness of their employees' use of the Internet. This includes the acceptability of Internet sites visited and the determination of personal time versus official work hours.

III. USE

A. Internet access can provide significant performance benefits for the Agency. However, there are significant legal, security, and productivity issues related to Internet use. **EXAMPLES**:

1. Transmitting computer viruses and malware from Internet sources.

2. Consuming limited disk storage space with downloaded information from the Internet onto FSIS network drives and users' computers.

3. Eavesdropping of employees transmissions by hackers (**example**: this might include passwords, sensitive data, or correspondence).

4. Breaching data security, confidentiality, and intellectual property rights.

B. Computer equipment use and Internet access to accomplish job responsibilities has priority over personal use.

C. Employee participation during non-work hours in news groups, chat sessions, and e-mail discussion groups is permitted if these sessions have a direct relationship to the user's job. If personal opinions are expressed, a disclaimer stating that this is not an official position of the Agency must be included.

D. Video and voice files should only be downloaded from the Internet when they serve an approved Agency function.

E. Personal files obtained via the Internet may not be stored on FSIS networks.

IV. WIRELESS POLICY

FSIS employees in official travel status or telecommuting may use wireless Internet access services provided the following conditions are met:

A. Employees must use GOE when accessing the FSIS network.

B. The Government incurs no additional expense.

C. VPN client must be activated and used when accessing the FSIS network.

D. Internet Service Provider access software not authorized by OCIO cannot ■ be installed on the Government issued computer.

E. Virus and malware protection must be up-to-date. ■

■

PART SIX—E-MAIL GUIDANCE

I. GUIDANCE

Employees using Government-owned or -leased equipment consent to security monitoring, for incidental and personal uses, whether authorized or unauthorized. There is no privacy or confidentiality when using Government e-mail systems. E-mail messages are departmental property, not personal property. Privacy and confidentiality are expectations that do not apply to e-mail messages (stored, retrieved, or exchanged).

A. FSIS provides an e-mail system to enhance productivity. E-mail messages must:

1. Meet the same standards for distribution or display as if they are tangible documents or instruments.

2. Not contain messages, postings or materials that serve to abuse, insult, intimidate, threaten or harass others. Do not send e-mails to create an intimidating, hostile, or offensive environment.

3. Clearly and accurately identify the sender.

4. Not conceal or misrepresent the sender's name or affiliation in an effort to dissociate the sender from responsibility for their action. It is inappropriate to alter the e-mail source, message, or posting.

5. Ensure the following information is shown in the signature line of all e-mail messages sent, replied to, or forwarded:

a. Name and title.

b. Department, Agency, division, and branch.

c. Mailing address.

d. Telephone number, facsimile number, and e-mail address.

B. Do not access any mailbox other than your own without authorization. If circumstances arise and someone else's mailbox requires access, submit a request for authorization to the Information System Security Program Manager, OCIO via Outlook at OCIO Security Operations Center.

C. Remain sensitive to inherent limitations of shared network resources. No computer security system can prevent a determined person from gaining unauthorized access to sensitive information. The Agency cannot guarantee electronic document privacy and confidentiality.

D. Ensure you know and understand the guidelines and policies of an electronic message board or social media site before sending or replying to a message. If you subscribe to an electronic discussion list, or set up a social media account, always ensure that you know how to unsubscribe from that list, and do so when you no longer have use for the information.

E. Refrain from forwarding e-mail messages without a legitimate business purpose under circumstances likely to:

1. Embarrass the original sender.

2. Violate the sender's clearly expressed desire to restrict additional dissemination.

F. Do not use e-mail to violate FSIS policy, regulation, or the rights of another. This abuse is subject to restricted e-mail and network access privileges and appropriate disciplinary action.

G. Do not put Government telecommunication systems to uses that would reflect adversely on USDA or FSIS. Such uses that could reflect adversely are:

1. Pornography.

2. Playing on-line games.

3. Private business.

4. Chain letters.

5. Unofficial advertising, soliciting, or selling except on authorized bulletin boards established for such use.

6. Violations of statute or regulation.

7. Inappropriately handled sensitive information.

8. Gambling.

9. Hate-oriented sites.

10. Other uses that are incompatible with public service.

H. Do not overburden the telecommunications system (such as sending broadcasts and group meetings).

I. Exercise caution when sending large messages to lists that may have hundreds of employees, and refrain from repeatedly sending or forwarding large messages or files (such as pictures or large attachments greater than 500 kilobytes) that will overburden the network.

II. E-MAIL RETENTION

A. Conserve the e-mail system. Be responsible for the content and maintenance of your e-mail box.

1. Check your e-mail frequently.

2. Delete unwanted messages immediately since they consume disk storage.

3. Keep retained e-mail messages in your e-mail box to a minimum.

4. Reduce the use of attachments when possible and enter the text directly into the e-mail message to eliminate additional steps.

5. Archive your messages by moving them from your mailbox to an Outlook personal storage folder file (.PST). To create an Outlook Personal Folder (PST File), from your inbox:

a. Click Tools, Options, Mail Setup Tab.

b. Click the Data files button.

c. Click the Add button.

d. Highlight Office Outlook Personal Folders File (.pst) and click OK.

e. In the Create or Open Outlook Data File window, type a descriptive name for the personal folder (or accept the default name). Click OK.

f. In the Create Microsoft Personal Folders window, type a descriptive name for the personal folder (or accept the default name). Click OK.

g. Click Close.

h. Click OK. (**NOTE**: The personal folder should appear in your Folder List window on the left side of the screen.)

6. Store the .PST file on your computer hard drive and save a backup copy on a DVD or flash drive.

B. OCIO uses a departmentally recognized process that follows DR 3080-001 to store all incoming and outgoing e-mail that transverse the FSIS network.

III. AUTOMATICALLY FORWARDED E-MAIL MESSAGES

A. FSIS does not permit auto-forwarding mail sent to your Agency e-mail

address box.

B. Reasons for not permitting auto-forwarding include:

1. Carelessness in creating and managing mailbox-forwarding rules can cause significant harm to the server and result in the loss of e-mail service to employees.

2. FSIS uses the *fsis.usda.gov* mail address to document official communication. FSIS employee e-mail addresses are registered to the FSIS e-mail directory, which enables traceability. In a dispute, e-mail that is auto-forwarded out of the FSIS domain cannot be used to defend a complaint against the Agency.

IV. IM

IM encompasses peer-to-peer applications that pose a significant threat to the FSIS network. IM use and downloading are prohibited on GOE. (See DM-3525-002.) Peer-to-Peer software and other programs that perform IM functions have no departmental business need and must not be loaded on workstations or equipment used to conduct official USDA business.

V. MULTI-RECIPIENT E-MAILS

Guidelines for approval when requesting a multi-recipient e-mail message.

A. Examples of what can be included:

1. Departmental issuances such as event announcements, street closings, shuttle service, or fire drills.

2. Health service messages such as blood testing and Employee Assistance Program services.

3. Federally sponsored groups.

4. Fliers for employees retiring or leaving the Agency.

B. Examples of what cannot be included:

1. Ads for sale of items.

2. Leave donor requests.

C. Identify the following information with the request:

1. Before submitting a request for approval, classify the message as:

a. Announcement.

b. Memorandum.

c. Event.

d. Informational.

e. Reminder.

2. Submit a Footprints ticket at http://service/footprints to publish an announcement. If the message contains special formatting, attach the text (**example**: Word document) to the Footprints ticket. **Do not** type the message text directly in the Footprints ticket.

3. Allow 1 full business day when requesting to publish an announcement.

4. Provide a contact for replies in the message.

5. Provide the subject and corresponding text for all entries.

6. Limit the use of attachments, whenever possible. If an attachment contains just text, cut and paste it into the message body.

D. Provide the distribution list(s) of recipients to receive the message (**example**: All Users).

1. Review text for typographical errors.

2. State whether or not there is an attachment.

3. Keep graphics to a minimum.

4. Total message size must be less than 500 kilobytes. The size of a message can be determined by adding the 'Size' column header to your existing Inbox column header row. From your Inbox:

a. Put the cursor on top of the 'From" column header and right click once.

b. Click on "Customize Current View."

c. Select "Fields."

d. Select "Size" from the Available Fields column.

e. Select "Add" and click OK.

E. Use the following standards for all broadcast messages:

1. Font – Sans Serif.

2. Font Size – 12.

3. Font Color – Black.

VI. MULTI-EMPLOYEE DISTRIBUTION LISTS

Users may send to distribution lists for their own program area. (**EXAMPLE**: OM users can send to the OM list or to any OM division distribution list.) However, OM users cannot send to any other program area or divisional lists (**example**: OFO).

VII. E-MAIL SIZE CONSTRAINTS AND CONTENTS

To manage the distribution of available resources within FSIS' network, the following is required:

A. Except for multi-recipient e-mail messages, messages must be less than 20 MB in size. Some field employees use dial-up access and downloading large documents is problematic.

B. Documents in any standard software package are acceptable (**examples**: Word, Excel, etc).

C. Messages should be straight text without graphics. Do not add signature images or logos. Use /s/ rather than a signature image. **NOTE**: Some users access e-mail via personal electronic devices that can only view Microsoft and Excel documents.

D. Do not use color, pictorial, or animated backgrounds in your messages.

E. Animated icons called Emoticons contain Spyware. Never download or add animated Emoticons to your e-mail messages.

F. Use Portable Document Format files to assure that employees do not alter file contents.

PART SEVEN—REIMBURSEMENT POLICY FOR BROADBAND SERVICES

I. POLICY

It is FSIS policy to:

A. Restrict access to the FSIS network from EOE. EOE connected to the FSIS network is not authorized or supported.

B. Deny reimbursement for employees' additional telephone lines of broadband connection costs unless covered under paragraph III.

C. Deny broadband reimbursement for employees with Blackberry™ tethering capability or who have EVDO wireless cards.

II. AGENCY RESPONSIBILITIES

The Agency:

A. Ensures that FSIS-approved computer software and security patches are applied correctly.

B. Supports a direct-wired or broadband card connection between broadband services and FSIS-owned computers. (**NOTE**: The Agency, including the FSIS Service Desk, will not support the use of EOE, routers, or services used as part of a home network.)

C. Reviews, approves, and submits the completed SF-1164 within 45 calendar days for payment. (See paragraph IV.)

III. ELIGIBILITY FOR BROADBAND REIMBURSEMENT

Reimbursement of broadband costs will be provided by OCIO only for the following employees:

A. SES.

B. Recall management staff.

C. Headquarters – level COOP only.

D. EMC (maximum of three employees per program area).

E. OPACE (maximum of three recall employees).

IV. REIMBURSEMENT PROCEDURES

A. **Reimbursement Requests**. Approved employees (see paragraph II.) must be submitted within 60 calendar days after the end of the quarter.

B. **Reimbursement Submission**. Approved employees (see subparagraph III.) must complete an SF-1164 and attach the original cable, modem, or DSL bill. If unable to locate and send an original bill, obtain a copy, sign and date it, and include the statement "in lieu of original" on it. Send the SF-1164 and the bill(s) to:

USDA FSIS OFFICE OF CHIEF INFORMATION
OFFICER (OCIO)
ROOM 4452 SOUTH BUILDING
1400 INDEPENDENCE AVENUE SW
WASHINGTON DC 20250–3700

C. **Reimbursement Criteria**.

1. Reimbursement is limited to eligible employees that have DSL or cable modem broadband connectivity. The reimbursement charges only include the service charge and rental fees for the modem. The total reimbursable charge cannot exceed $70 per month.

2. Only one startup installation charge will be reimbursed per employee, per year, except on a case-by-case basis with prior OCIO approval.

3. Either Blackberry™ tethering or wireless card services are provided, if available, in lieu of reimbursement for broadband service.

4. Reimbursement will not be permitted if tethering or wireless cards are provided to employees.

V. RESTRICTIONS FOR EOE

A. EOE connected to federally reimbursed broadband is permitted for personal use, if the broadband use:

1. Involves no additional expense to the Government.

2. Does not violate security policies or pose a security risk for the Agency.

3. Does not interfere with official business.

B. EOE can never be used to connect to the FSIS network.

PART EIGHT—FSIS WIRELESS SERVICE ACQUISITIONS

FSIS promotes the most cost-effective use of commercial wireless mobile communications and encourages coordinated acquisition planning and shared usage plans to reduce costs where feasible.

I. ELIGIBILITY FOR WIRELESS SERVICE FUNDING OR REIMBURSEMENT

A. OCIO only funds or reimburses Blackberry™ tethering or EVDO wireless card service costs for the following employees:

1. SES.

2. Recall management staff.

3. Activated headquarters-level COOP and Crisis Action Team personnel.

4. EMC (maximum of three employees per program area).

5. OPACE recall leads (up to three employees).

6. Designated OCIO personnel.

B. Program areas are responsible for funding Blackberry™ tethering or EVDO wireless card service costs for the following employees:

1. Non-activated headquarters-level and COOP personnel.

2. All other roles and staff.

II. APPLICABILITY

Part Eight of this directive applies to all:

A. Commercial wireless devices, services, and technologies that transmit voice and data.

B. FSIS employees authorized to use EVDO communications or Blackberry™ tethering capability for business operations.

III. **PROVISIONS**

A. The program area:

1. Provides funding for Blackberry™ tethering or EVDO wireless service costs requested for their employees. (**NOTE**: There is a limited activation of three EVDO cards per day. This ensures that the FSIS service desk team can effectively manage callers requiring EVDO activation assistance.)

2. Must immediately report lost or stolen EVDO cards by following the instructions under Part One, subparagraphs VI. G. and H. Service provided for lost or stolen EVDO cards will be terminated.

3. Must immediately request cancellations for EVDO card service by creating a Footprints Request ticket via the Intranet at http://service/footprints.

B. The TB:

1. Maintains a loaner pool of 10 EVDO cards (cards without service). Service is activated on loaner EVDO cards on an as-needed basis. EVDO loaner cards are funded by OCIO. Requests for loaner cards require CIO approval prior to issuance. The maximum time limit for a loaner EVDO card is 30 days.

2. Terminates service provided for lost or stolen EVDO cards.

3. Orders new and replacement EVDO cards.

IV. **ACQUISITION JUSTIFICATION**

A. Supervisors must ensure that the service procured is justified, technically effective, appropriately managed, and meets one of the following criteria:

1. An employee who works 3 or more days per week away from their fixed office (**example**: frontline supervisors).

2. A member of the Recall Management Staff.

3. A member of the EMC.

4. An employee who is in a service capacity and must be accessible 24 hours a day, 7 days a week.

B. Employees who meet at least one of the criteria listed in subparagraph IV. A.1-4 and have been issued a Blackberry™ (previously funded by the program office) will be offered Blackberry™ tethering. An EVDO card will be ordered if the tethering service feature is not available through the Blackberry™ device.

V. PROCEDURES FOR OBTAINING SERVICES WHEN FUNDED BY THE PROGRAM AREA

Requests for program funded commercial EVDO or Blackberry™ tethering communication services for employees are processed as follows:

A. The program area office prepares a completed Form AD-700. Include the following information on the AD-700:

1. Name of the employee requiring the service.

2. Type of service requested (EVDO card or tethering).

3. Work and home address of the employee requiring the service.

4. Estimated monthly cost for the service requested.

5. Management code used to fund the monthly service.

6. Provide justification for service requirement that meets one of the criteria listed in subparagraph IV. A. 1-4.

B. The program area office submits a completed Form AD-700 to the TB, OCIO, via fax at 202–690–3738, or scans and e-mails to TelecommunicationsTeam@fsis.usda.gov. (**NOTE**: The cost of the service must be paid by the requesting program area office.)

C. A service provider will be selected by the TB based on the best available service coverage.

VI. PROCEDURES FOR OBTAINING SERVICES WHEN FUNDED UNDER THE PUBLIC HEALTH DATA INFRASTRUCTURE CONSOLIDATION SYSTEM

Requests for commercial EVDO services and cards for OFO fixed and patrol inspection assignments are processed as follows:

A. As new assignments are established, the RMS within each OFO DO must submit requests by creating a Footprints Request ticket via the Intranet at http://service/footprints.

B. The RMS must provide the following information in a Footprints Request ticket:

1. Assignment number associated with the EVDO service or card request.

2. Address for each establishment covered within the assignment number.

3. Name of the Federal inspector working the assignment number.

4. Whether the location is a fixed establishment location or patrol assignment.

C. The DO must issue only one EVDO card per fixed establishment location or patrol assignment.

D. The EVDO cards will be shipped to the requesting DO address.

E. The requesting RMS will deliver the EVDO card to the FSIS inspector and update the FSIS Microsoft SharePoint Web site with all changes to the EVDO card assignment database.

F. The RMS will report patrol or fixed assignments that become vacant by creating a Footprints Request ticket. EVDO services for assignments remaining vacant for more than 30 days will be suspended until the vacancy is filled by the DO. The DO will maintain the EVDO cards that have suspended service.

VII. ACTION BY THE TB

The TB:

A. Processes the AD-700 within 3 business days.

B. Activates the tethering feature within 72 hours after the AD-700 is approved.

C. Creates and sends a Footprints Request ticket to the employee when the tethering feature is activated. The ticket will contain the installation instructions to launch the tethering service on the Blackberry™ device. For additional assistance, the employee can reply to the Footprints Request ticket requesting assistance.

D. Updates the FSIS SharePoint Web site with changes to the EVDO card assignment database.

E. Verifies the availability of the requested service at the location specified on the AD-700.

F. Ships EVDO cards to the requesting office address provided on the AD-700.

VIII. ADDITIONAL INFORMATION

FSIS continues to progress in replacing computer dial-up connections used by FSIS field personnel with high-speed telecommunication lines. (**NOTE**: Not all food production establishments are located in areas that have ready-access to hard-wired, high-speed services. For those locations, FSIS is implementing EVDO mobile wireless broadband service where available.)

A. Provisions for FSIS field EVDO services under the Public Health Data Infrastructure Consolidation System are:

1. Limited to Federal inspection locations or assignments.

2. Only available to Federal employees in OFO working at fixed establishment locations or on patrol inspection assignments.

B. The goal of the Public Health Data Infrastructure Consolidation System broadband sites is to provide one dedicated Internet connection, replacing dial-up at fixed establishment locations or one location on patrol inspection assignments.

Assistant Administrator
Office of Management

DEFINITIONS

A. **Animated Icons or Emoticons**. A small picture like an object or program such as a smiley or an emotion to convey a tone or attitude in computerized e-mail communication with lifelike movement or an animated cartoon form.

B. **Bluetooth**. A short-range radio technology aimed at simplifying communications among Internet devices, between devices and the Internet, and simplifies data exchange between Internet devices and other computers.

C. **Broadband**. Telecommunication term for Internet connection (cable, modem or DLS service) in which a wide band of frequencies are available to transmit information.

D. **Chain E-mail**. A letter circulated among many people sent electronically, copied, and then passed to others with a request to do the same.

E. **Commercial Activity**. An activity that is for commercial (or "for-profit") purposes such as outside employment or support of a personal private business activity (**examples**: consulting for pay, sales, or administrating business transactions, or the sale of goods or services).

F. **Computer Equipment**. Any equipment interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. **EXAMPLES**: Computers, ancillary equipment, software, firmware; and similar procedures, services (support services) and related resources.

G. **DSL**. High-speed digital data technology that provides digital data transmission over the wires of a local telephone network.

H. **Emergency Responders**. Staff officials designated for on-call operations support or emergency response.

I. **Employee**. An individual currently working for FSIS, whether full-time, part-time, intermittent, or on a contract basis.

J. **Enterprise Architecture**. A comprehensive framework used to manage and align an organization's IT assets, people, operations, and projects with its operational characteristics.

K. **Ethernet**. A local-area network. Ethernet uses a bus or star topology and supports data transfer rates of 10 megabytes per second.

L. **EVDO Cards**. A telecommunications standard that uses radio signals in data transmissions for wireless devices, services, and technologies that transmit and receive voice and data. Laptop computers typically use PC card ports and Blackberry™ devices utilize cable tethering for EVDO card connections.

M. **Extranet**. An extension of an organization's Intranet out onto the Internet, available to selected customers to exchange information.

N. **FIPS 140-2**. A U.S. Government computer security standard used to specify requirements and accredit cryptographic (the practice of hiding information) modules.

O. **FireWire®**. A peripheral (port, wire, card, etc.) that allows high-speed devices, such as digital camcorders, audio recorders, and external storage to connect to computers.

P. **Flash Drives**. Portable flash memory cards that plug into a computer's USB port and functions as a portable hard drive. USB flash drives are also referred to as pen drives, key drives, or USB drives.

Q. **For-Profit Activity**. An activity that is "for-profit" (or commercial) purposes such as outside employment or support of a personal private business activity (**examples**: consulting for pay, sales, or administration of business transactions, or the sale of goods or services).

R. **Host**. A computer system that is accessed by a user working at a remote location. Typically, the term line is used when there are two computer systems connected by modems and telephone.

S. **IM**. A form of "real time" communication between two or more people based on typed text conveyed via devices connected over a network, such as the Internet.

T. **IT Resources**. A collection of computing and/or communications components and other resources that support one or more functional objectives of an organization.

U. **Information Systems**. Any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

V. **IT**. Computing, communications hardware, or software components and related resources that can collect, store, process, maintain, share, transmit or dispose of data. IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software.

W. **Infrared**. Short for Infrared Data Association, a group of device manufacturers that developed a standard for transmitting data via infrared light waves. Computers and other devices such as printers come with infrared data access ports, which enable data to be transferred from one device to another without any cables.

X. **Internet**. A worldwide network of computer networks that use the network protocols to facilitate data transmission and exchange. Anyone with a computer can access the Internet through an Internet Service Provider.

Y. **Intranet**. A network belonging to an organization and accessible only by the organization's members, employees, or others authorized to share information. The Agency's Intranet is known as "Inside FSIS."

Z. **Inventory Control**. A detailed list of equipment in one's possession.

AA. **Inventory Control Officer**. An individual who has the responsibility of making and maintaining a detailed list of equipment.

BB. **License**. A contract that grants FSIS explicit rights to use intellectual property.

CC. **Malware**. Malicious software, such as a virus that is designed to specifically damage or disrupt a system.

DD. **Media**. Objects that store data. These include hard disks, floppy disks, CD-ROMs and tapes.

EE. **Napster**. An application that gives individuals access to one another's audio files by creating a unique file-sharing system via the Internet.

FF. **Network**. An interconnection of a group of computers. Computer networks can be classified according to their scale (**examples**: LAN and WAN). Computer networks can also be classified according to the hardware technology that is used to connect the individual devices in the network (**examples**: optical fiber, ethernet, wireless LAN, or power line communication).

GG. **Network System**. A group of two or more computer systems linked together. Local-area networks and wide-area networks are two examples of networks.

HH. **Patch**. A quick-repair job for a piece of programming. A patch (sometimes referred to as a "fix") is an immediate solution users may download from the software maker's Web site.

II. **PDA**. A handheld device (**example**: Blackberry™ device) that combines computing, telephone or fax, Internet and networking features. PDAs can function as a cellular phone, fax sender, Web browser and personal organizer.

JJ. **Peer-to-Peer Software**. Software programs that can link your computer to other computers across the Internet to share files, music, and videos.

KK. **Personal Files**. Stored data not referring to FSIS business.

LL. **PII**. Informtion that can be used to distinguish or trace your identity. Examples include your social security number or medical records, or information that, when combined or used with other identifying information, is linked or linkable to a specific individual.

MM. **Plug-in**. A hardware or software module that adds a specific feature or service to a larger system. The idea is for the new component to plug into the existing system.

NN. **Portable Electronic Device**. A palm sized computing device that provides users with wireless connection to e-mail, Internet and voice communications.

OO. **Portable Electronic Device Server**. A dedicated computer or device on a network that manages portable electronic device resources.

PP. **Program Area**. Any of the nine FSIS program offices and the Office of the Administrator.

QQ. **Property Record**. A tracking mechanism to record information, such as the manufacture, model number, serial number and the assigned user.

RR. **Routine Operations**. A regular, customary process or action that is a series of some work.

SS. **SSL**. A software object that connects an application to a network protocol.

TT. **Standard Image**. The standard software package that is loaded on all FSIS computer equipment and is supported by OCIO. Games such as solitaire, hearts, etc., are included as part of the FSIS standard software image with the intention that the games will be used during personal time as a learning tool to navigate the mouse during personal time.

UU. **TCCB**. The forum that manages and monitors the Systems Development Life Cycle for the Agency and the impact of changes to an IT system.

VV. **Tethering**. Connecting a non-mobile device with a mobile one for the purpose of wireless Internet access.

WW. **User**. An employee that uses a computer.

XX. **Virus**. A program or piece of code that is loaded onto a computer without permission or approval. Viruses can replicate themselves and are dangerous because they quickly use all available memory and cause system failure. A more dangerous virus is one capable of transmitting itself across networks and bypassing security systems.

YY. **VPN**. A technology by which authorized individuals can gain access to a organization's intranet via the Internet.

ZZ. **Web Browser**. A software application used to locate and display Web pages. Modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

AA. **Wireless Connection**. Communication without wires.