U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	**Number:** DR 3580-003
SUBJECT: Mobile Computing	**DATE:** September 24, 2013
	OPI: Office of the Chief Information Officer

1. PURPOSE

This Departmental Regulation (DR) defines the requirements for the control of information accessed or stored by mobile computing and storage devices. This policy also facilitates the management of mobile computing risk by providing guidelines to ensure that:

a. United States Department of Agriculture (USDA) mobile computing assets are appropriately managed, and secured;

b. The confidentiality, integrity and availability of USDA sensitive information is secured while at rest or in transit; and

c. Mobile users are properly trained and aware of their responsibilities.

This policy refers to and enhances existing USDA policies including, but not limited to: privacy, remote access, encryption, and sensitive but unclassified (SBU) information protection. All applicable policies should be read to ensure a full

understanding of Departmental and Federal requirements, directives, mandates, and standards.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This DR will be in effect until superseded. If a specific provision of this DR is superseded or otherwise invalidated by external mandate, USDA directives, or standards, such guidance does not invalidate the remainder of this DR.

b. In this directive, the terms "directive," "DR," and "policy" may be used interchangeably.

c. This policy does not apply to or address classified information or communications. Classified information or communications shall be handled in accordance with policy and guidance issued by the USDA Office of Homeland Security and Emergency Coordination (OHSEC).

3. APPLICABILITY AND SCOPE

a. This DR applies to all USDA agencies, offices, and personnel working for or on behalf of USDA. References to "personnel," "users," or "employees" throughout this policy shall be interpreted to include all active (non-terminated) employment status USDA federal and non-federal (contractors, partners, affiliates, volunteers, et al.) employees who have an identity in the USDA's authoritative identity management system and are authorized to use mobile devices and access USDA resources, information, and data.

b. This policy applies to any government furnished mobile computing device, technology, resource, or service that:

(1) Is owned or managed by USDA;

(2) Is connected to a USDA network;

(3) Connects to another Federal government technology resource or service; or

(4) Stores USDA and other Federal government data or information.

c. This policy applies whether the network connections are remote or via the trusted network.

d. This policy applies to USDA and Federal government information that exists in a digital format that is accessed remotely or resides on a mobile device, whether stored in a database or used in an application.

e. This policy does not apply to or address non-Government furnished equipment (non-GFE) or Bring Your Own Device (BYOD) programs and initiatives. Separate BYOD guidance will be issued by the Office of the Chief Information Officer (OCIO).

4. BACKGROUND

In this era of mobile computing, powerful hand-held devices, wireless communications, cloud services, and social networks are creating new business delivery opportunities for USDA. Federal government agencies shall embrace this technology and be ready to mobilize their business, transform their organizations, and modernize their technical infrastructures to meet the significant opportunities as well as challenges that mobility brings to the federal workplace.

Responding to today's mobile opportunities requires that USDA not only embrace and support the use of these new devices and technologies, but also manage and secure them. Mobile device and application management tools and end point management tools provide the capabilities to secure, monitor, manage and support mobile devices. The mobile application management functionality typically includes: inventory management; monitoring; administration; over-the-air (OTA) distribution of applications; and data and configuration settings for all types of mobile devices, including mobile phones, smart phones, tablet computers, mobile wireless fidelity (WiFi) hotspots, and laptops for Government furnished equipment (GFE).

USDA's implementation of mobile device and application management tools will supplement and extend existing computer management capabilities beyond the traditional infrastructure and optimize the functionality and security of mobile devices in our workforce while minimizing cost and downtime.

5. POLICY

a. All USDA hardware, software, and mobile devices connected to the USDA network shall be handled in accordance with NIST standards and checklists, as well as any other applicable federal laws, regulations, and standards. Configuration checklists and standards can be found on the NIST National Vulnerability Database. If USDA or NIST standards are unavailable, industry best practices shall be used until NIST standards are issued.

b. All USDA owned and managed mobile computing devices and associated data are subject to electronic discovery (eDiscovery) for business purposes. In some cases, the devices may be physically collected to retrieve data and returned at a later date.

c. Users are required to sign an AD-3051, *Acceptable Use Policy Agreement* (AUPA) and AD-3052 *Rules of Behavior* (ROB) form when assigned a mobile device. These forms are available electronically on the USDA Forms Management Web site. Agencies may add more stringent requirements to the baseline AUPA and/or ROB agreements, but may not weaken the baseline requirements described in AD-3051 and AD-3052.

d. Mobile computing devices authorized to connect to USDA's trusted network must be registered and managed by the USDA's mobile device management (MDM) tool. Application authorization must be managed by an approved Departmental or agency tool.

e. Every end user shall adhere to USDA de-provisioning requirements stipulating actions to be taken upon termination of employment or loss of eligibility, as identified in DM 3300-005, "Policies for Planning and Managing Wireless Technologies in USDA."

f. In accordance with existing USDA privacy agreements, federal laws, and regulations, an employee's government furnished mobile devices, their contents, and related transmissions, including but not limited to: text messages, digital photos, and files may be monitored, intercepted, searched, recorded, and seized.

g. USDA reserves the right to assess whether and which mobile devices meet the Department's established security standards.

h. USDA reserves the right to refuse connection of any mobile device to the USDA trusted network that does not meet applicable USDA security guidelines, policies, or NIST standards.

i. Should it be determined that any device is using the network inappropriately, network traffic to and/or from that device may be monitored or terminated by USDA.

j. USDA reserves the right to disconnect any resource from the network until suspected security incidents can be resolved.

k. International travel poses additional risk to mobile technology being utilized while on travel status. Users must be aware and understand that they are subject to the laws of the visited country, there is no expectation of privacy in most countries, and wireless devices are particularly vulnerable to interception and malware infection.

l. The following measures shall be complied with for Government furnished mobile devices used domestically or internationally:

(1) Strong passwords as determined by USDA/[agency] security policy shall be utilized.

(2) Mobile devices must have up-to-date antivirus, antispyware, security patch, and firewall software installed and running with the most stringent settings possible if they are capable of supporting these technologies and/or applications.

(3) Unneeded and unnecessary features shall be disabled. The list of unneeded/unnecessary features is ever changing and tends to be specific to the business need; therefore, agencies are responsible for identifying the features to be disabled.

(4) All sensitive information stored, transmitted or viewed on mobile devices and removable media shall be protected and encrypted in accordance with DR 3440-002, "Control and Protection of Sensitive Security Information," DM 3550-002, Chapter 10, Part 2, "Sensitive But Unclassified (SBU) Information Protection," and DR 3170-001, "End User Workstation Standards," Appendix B, Section 16.0, "Portal and Mobile Devices."

(5) Mobile devices and removable media shall not be transported in checked baggage.

m. Government furnished mobile devices used for international travel shall be prepared as follows:

(1) Agencies and Offices shall consult with Office of Homeland Security Emergency Coordination (OHSEC) for current precautions to be observed for destination countries prior to departure.

(2) Government furnished mobile devices and removable media used domestically shall not be used while on international travel, unless the agency has documented approval and accepted the risk for the use of this equipment.

(3) Government furnished mobile devices and removable media will only be used in the performance of officially sanctioned travel. If the devices are not essential to the mission, the equipment shall not be taken.

(4) Agencies shall document approval and acceptance of risk for any GFE including, but not limited to, mobile devices and removable media allowed to be used during personal travel.

(5) Approved GFE for use while on international travel shall be decommissioned or reformatted (wiped) immediately upon return.

(6) The servicing Information Technology (IT) unit shall make a copy of all mobile device profiles, including but not limited to: operating system, configuration, and signatures for system and applications used on the device. This "snapshot" shall be used to evaluate any possible changes made to the device upon return to the office.

(7) All sensitive information needed for the mission shall be encrypted per DR 3170-001, Appendix B, Section 16.0 "Policy" if encrypted devices are allowed by the country(s) being visited.

n. Agencies shall ensure training/education materials pertaining to the appropriate use of mobile devices and removable media while on international travel is provided to users prior to official international travel taking place.

o. Users shall exercise a higher level of due diligence in the protection of mobile devices while on international travel than would be expected in the domestic environment.

(1) Whenever possible, mobile equipment shall be powered off and the batteries/subscriber identity module (SIM) cards removed and stored separately from the device when not in use to minimize the opportunity for unauthorized access or misuse by foreign entities.

(2) Bluetooth capability shall only be enabled and used if absolutely necessary for the performance of the mission, as identified in NIST SP 800-121, "Guide to Bluetooth Security." Bluetooth usage is restricted to USDA-issued headsets and earpieces; Bluetooth hands-free automobile speaker usage is prohibited.

(3) Foreign thumb drives, compact disks (CDs), or other media shall not be used in USDA mobile equipment. If such use cannot be avoided, the mobile device shall be assumed to be compromised and shall be decommissioned and/or reformatted immediately.

(4) USDA mobile devices and removable media shall not be used with or in foreign equipment due to the possibility of compromise.

(5) Public Internet kiosks, cafes, business centers, and hotel WiFi sites are particularly susceptible to monitoring, data interception, and control by foreign entities. Transmission, storage, or printing of sensitive government and personal information is prohibited unless these actions take place in a prescribed manner and in a pre-approved, secure location:

(a) Encrypt all transmissions if allowed by the country(s) being visited. Protect sensitive and personal information transmissions per the requirements of Section 5(l)(4). Potential solutions for international

information transmission include: (1) USDA in-country office location, (2) U.S. Embassy location, (3) U.S. Consulate location, and (4) other U.S. Government in-country office or approved telecommunications services location, and (5) portable printer.

(b) Store all data files in encrypted form per the requirements of Sections 5(l)(5) and 5(m)(7).

(c) View or print all data files per the requirements of Section 5(l)(5). Potential solutions for international printing include: (1) USDA in-country office location, (2) U.S. Embassy location, (3) U.S. Consulate location, (4) other U.S. Government in-country office or approved printing location, and (5) portable printer.

(6) If a mobile device is lost or stolen while on international travel, the loss must be reported to the agency's or Department's incident response team and the local U.S. embassy or consulate immediately upon detection/discovery.

p. Upon return to USDA after international travel, the government furnished mobile devices:

(1) Must be turned off or not used domestically until the mobile device(s) can be examined by the appropriate IT staff to ensure the mobile device has not been modified or infected by malicious code.

(2) Shall not connect to any USDA servers or networks for any reason prior to this examination.

(3) Shall have device passwords changed upon return to the United States (U.S.).

6. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) shall:

(1) Establish policies, procedures, and guidance on mobile computing;

(2) Enforce the policy through compliance reviews, automated tools, and other means necessary;

(3) Ensure mobile device training is integrated into existing workforce education and training programs to ensure employees receive information security awareness and ROB training; and

(4) Direct agencies and staff offices to comply with this regulation and monitor employee compliance.

b. Agency and Staff Office Chief Information Officers (CIO) shall:

(1) Implement this policy within their respective agency and staff offices;

(2) Provide evidence of compliance upon request;

(3) Ensure mobile computing user agreements and ROB documents are in compliance with agency or office information security policies;

(4) Allow only secure remote data access methods (as identified in DR 3180-001, "Information Technology Network Standards" and in the applicable 3500 series of directives), and as approved by the USDA CIO in support of mobile users;

(5) Direct that no sensitive or personally identifiable information (PII) data resides on any mobile device unless protected as required and approved in advance in writing as identified in DR 3180-001 and DM 3550-002;

(6) Direct every end user to abide by the compliance rules and regulations established in Section 5 of this DR, which includes policies or configurations that have been implemented on their authorized USDA owned or managed devices connecting to USDA and Federal government networks;

(7) Ensure data that has been authorized to be stored on a mobile device is:

(a) The minimum data necessary to perform the business function;

(b) Stored only for the time needed to perform the business function;

(c) Encrypted using methods authorized by current Federal standards for data in transit and data at rest (as identified in DR 3180-001 and in the applicable 3500 series of directives), when required;

(d) Protected from unauthorized access and disclosure; and

(e) Stored only on approved devices in accordance with USDA cyber security policies.

(8) Work with Office of General Counsel (OGC), Office of the Inspector General (OIG), and the Departmental Records Management Officer to help ensure that paper and electronic records and other non-record documentary

materials, including electronically stored information (ESI), are accessible for eDiscovery purposes;

(9) Coordinate all agency and staff offices Information Discovery and Litigation Support (IDLS) activities that require planning, coordination, and execution with related USDA offices for purposes of preserving and/or producing electronically stored information. IDLS activities consists of request(s) for preservation and/or production of electronic data (including related hardware retention) related to litigations, subpoena, Freedom of Information Action (FOIA), forensic investigations, and any other investigations and/or inquiries where electronic data are to be preserved and/or produced; and

(10) Ensure their agency and staff offices issue Standard Operating Procedures (SOPs) for the acceptable use of mobile devices (as identified in DM 3300-005).

c. Agency and Staff Office Supervisors shall:

(1) Direct individual users to comply with security and privacy guidelines and appropriately monitor user compliance;

(2) Direct individual users to abide by the compliance rules and regulations established in Section 5 of this DR;

(3) Keep all user's mobile computing agreements and rules of behavior documents on file; and

(4) Work with program, IT, and OGC staff to help ensure that paper and electronic records are accessible for eDiscovery purposes.

d. Federal and Non-Federal Employees shall:

(1) Complete the mandatory annual USDA Information Security Awareness training prior to being permitted access to the USDA network or assigned a mobile device;

(2) Abide by the compliance rules and regulations, established in Section 5 of this DR, which includes policies or configurations that have been implemented on government furnished devices connecting to government networks;

(3) Not bypass or disable USDA installed security policies or configurations under any circumstances. Mobile devices that are jail broken, rooted, or unlocked are considered to be out of compliance with this policy and with NIST security configurations and will not be allowed to access USDA resources or information;

(4) Exercise due diligence in the protection of GFE including, but not limited to, protecting and securing GFE from loss, theft, and compromise. Mobile devices shall not be left unattended at any time, and employees shall take all reasonable and appropriate precautions to protect and control these devices from unauthorized physical access, tampering, and loss or theft;

(5) Immediately report loss, theft, or any compromise of Government furnished equipment to their supervisor and the appropriate incident response group. Failure to exercise proper care and protection of GFE may subject the employee to reimbursement costs or disciplinary action;

(6) Exercise due diligence and in the protection of government sensitive and PII data. The employee shall only connect to public WiFi hot spots in a secured manner, using a Virtual Private Network (VPN) or other USDA approved connectivity method to protect government data;

(7) Adhere to USDA de-provisioning requirements stipulating actions to be taken upon termination of employment or loss of eligibility;

(8) Maintain paper and electronic records and non-record ESI according to DR 3080-001, "Records Management," DR 3085-001, "Vital Records Management", DR 3090-001, "Litigation Retention Policy for Documentary Materials including Electronically Stored Information," and DR 3099-001, "Records Management Policy for Departing Employees, Contractors, Volunteers, and Political Appointees";

(9) Comply with USDA DM 3300-005 Chapter 3 guidance for limited personal use of GFE. Personal use is permitted on an occasional basis provided that the use does not interfere with official business and involves minimal expense to the Government. Occasional personal use of mobile device tools shall normally take place during the employee's personal or off-duty time; however, official Government business always takes precedence.

7. PENALITIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DM 3300-005, "Policies for Planning and Managing Wireless Technologies in USDA," Chapter 3, sets forth USDA's policies and standards on employee responsibilities and conduct relative to the use of wireless technologies.

DR 4070-735-001, "Employee Responsibilities and Conduct," Section 16, sets forth the USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of Computers and Telecommunications Equipment, with further delineation provided in DR 3300-001, "Telecommunications and Internet Services and Use," Section 3. In addition, DR 4070-735-001, Section 21, Disciplinary or Adverse Action, states:

a. A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action.

b. Disciplinary or adverse action shall be effected in accordance with applicable law and regulations.

Such disciplinary or adverse action shall be effected in accordance with applicable law and regulations such as the Code of Ethics for Government Employees, Office of Personnel Management (OPM) regulations, Office of Management and Budget (OMB) regulations, and Standards of Conduct for Federal Employees.

8. POLICY EXCEPTIONS

a. All USDA agencies and staff offices are required to conform to this policy; however, in the event that a specific policy requirement cannot be met as explicitly stated, agencies may submit a waiver request. The waiver request shall explain the reason for the request, identify compensating controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the policy requirement. Agencies and staff offices shall address all policy waiver request memorandums to the Associate Chief Information Officer (ACIO), Agriculture Security Operations Center (ASOC) and submit the request to cyber.communication@usda.gov for review and decision.

b. Unless otherwise specified, agencies shall review and renew approved policy waivers every fiscal year. Approved waivers shall be associated with a NIST security control and tracked as a plan of action and milestones (POA&M) item in the Department's FISMA data management and reporting tool. The ACIO-ASOC shall monitor and approve waivers.

-END-

APPENDIX A

DEFINITIONS

Acceptable Use: The ethical and allowable use of mobile computing devices at USDA. These acceptable use rules are in place to protect customers, business partners, and employees of USDA. Insecure practices and malicious acts expose USDA, customers, business partners, and employees to risks including, but not limited to, virus attacks, compromise of network systems and services, and loss of data or sensitive information. Security breaches could result in legal action for individuals or USDA. In addition, security breaches damage the USDA's reputation and could result in loss of services.

Discovery: Discovery is the process of identifying, locating, securing and producing evidence, including testimony, things, information, and materials for utilization in the legal process. The term is also used to describe the process of reviewing all materials which may be potentially relevant to the issues at hand and/or which may need to be disclosed to other parties, and of evaluating evidence to prove or disprove facts, theories or allegations. There are several formalized methods of conducting discovery, the most common of which are interrogatories, requests for production of documents and depositions.

Electronic Discovery (eDiscovery): The process of collecting, preparing, reviewing, and producing ESI in the context of the legal process. See Discovery.

Electronically Stored Information (ESI): Any information that is created, received, maintained or stored on local workstations, laptops, central servers, personal digital assistants, cell phones, or in other electronic media. Examples include, but are not limited to: electronic mail ("email"), calendars, word processing documents and spreadsheets, databases, videos, video files, digital images, audio files, text messages, voicemails, activity logs, etc. ESI includes metadata.

Information Discovery and Litigation Support (IDLS): Activities related to the preservation and/or production of electronically stored information for the purposes of electronic information discovery and litigation support.

Jail Breaking: Removing the limitations imposed on an Apple computing device, often through the installation of custom operating-system components or other third-party software. The equivalent action on an Android computing device is called "rooting."

Litigation Hold: The obligation of agencies, managers and individual employees to ensure that preservation of documentary materials in their native format that might be or might become relevant to pending or threatened litigation.

Mobile Computing: The term "Mobile computing" is used to describe the use of computing devices--which usually interact in some fashion with a central information

system—while away from the normal, fixed workplace. Mobile computing technology enables the mobile worker to: (a) create; (b) access; (c) process; (d) store; and (e) communicate information without being constrained to a single location.

Mobile Device: Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory). Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

Mobile Device Management: Refers to any routine or tools intended to distribute applications, data, and configuration settings to mobile communication devices such as cell phones, Portable Electronic Devices (PEDs), and Personal Digital Assistants (PDAs). It takes multiple types of mobile software and hardware to address a full solution. The intent of MDM is to optimize the functionality and security of mobile communications network, while minimizing costs and downtime.

Personal Use: An activity conducted for purposes other than accomplishing official or otherwise authorized business.

Records: All books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference and stocks of publications and of processed documents are not included.

Sensitive or Personally Identifiable Information (PII) Data: Includes but is not limited to:

- Personally identifiable information that is not in the public domain and if improperly disclosed could be used to steal an individual's identity, violate the individual's right to privacy or otherwise harm the individual;

- Organizational information that is not in the public domain and if improperly disclosed might: cause a significant or severe degradation in mission capability; result in significant or major damage to organizational assets; result in significant or major financial loss; or result in significant, severe or catastrophic harm to individuals.

- In accordance with the USDA policy and procedures, each agency is responsible for the assessment and categorization of their data in accordance with the definitions set forth in this policy.

APPENDIX B

ABBREVIATIONS

ACIO	Associate Chief Information Officer
ASOC	Agriculture Security Operations Center
AUPA	Acceptable Use Policy Agreement
BYOD	Bring Your Own Device
CD	Compact Disk
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CUI	Controlled Unclassified Information
DM	Departmental Manual
DR	Departmental Regulation
ESI	Electronically Stored Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
GFE	Government Furnished Equipment
IDLS	Information Discovery and Litigation Support
IT	Information Technology
MDM	Mobile Device Management
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
Non-GFE	Non-Government Furnished Equipment
OCIO	Office of the Chief Information Officer
OGC	Office of the General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OTA	Over-the-Air
PDA	Personal Digital Assistant
PED	Portable Electronic Device
PII	Personally Identifiable Information
P.L.	Public Law
POA&M	Plan of Action and Milestones
POS	Point-of-Sale
ROB	Rules of Behavior
SBU	Sensitive but Unclassified
SIM	Subscriber Identity Module
SOP	Standard Operating Procedure
SP	Special Publication
US	United States
U.S.C.	United States Code

USDA	United States Department of Agriculture
VPN	Virtual Private Network
WiFi	Wireless Fidelity

APPENDIX C

AUTHORITIES AND REFERENCES

Departmental Manual (DM) 3300-005, *Policies for Planning and Managing Wireless Technologies in USDA*, November 10, 2010

DM 3500-000, *Cyber Security Manual Series 3500 et seq*., July 14, 2004

DR 3505-002, *Wireless Networking Security Policy*, August 11, 2009

DM 3515-000, *Privacy Requirements*, February 17, 2005

DM 3545-001, *Computer Security Training*, February 17, 2005

DM 3550-002, *Sensitive but Unclassified (SBU) Information Protection*, February 17, 2005

Departmental Regulation (DR) 4070-735-001, *Employee Responsibilities and Conduct*, October 4, 2007

DR 4080-811-002, *USDA Telework Program*, January 25, 2011

DR 3080-001, *Records Management*, April 11, 2007

DR 3085-001, *Vital Records Management Program*, August 19, 2011

DR 3090-001, *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*, May 28, 2008

DR 3099-001, *Records Management Policy for Departing Employees, Contractors, Volunteers and Political Appointees*, July 02, 2012

DR 3140-002, *USDA Internet Security Policy*, March 7, 1995

DR 3170-001, *End User Workstation Standards*, December 12, 2007

DR 3180-001, *Information Technology Network Standards*, Appendix O, *Information Technology Network Security Standards*, September 30, 2008

DR 3300-001, *Telecommunications & Internet Services and Use*, March 23, 1999

DR 3300-1-C, Appendix C, *Wireless Communications*, March 23, 1999

DR 3440-002, *Control and Protection of "Sensitive Security Information,"* January 30, 2003

Executive Order 13011, *Federal Information Technology*, July 16, 1996

Federal Property Management Regulations, 41 C.F.R. §§ 101-102 (2013)

Freedom of Information Act (FOIA), 5 U.S.C. §552 (2013)

Government Paperwork Elimination Act, 44 U.S.C. §3504, et seq. (2013)

Information Technology Management Reform Act of 1996 (ITMRA; also known as the Clinger-Cohen Act of 1996), P.L. 104-106, February 1996

Paperwork Reduction Act of 1995, 44 U.S.C. §3501 et seq., (2013)

Federal CIO Council, *Recommended Executive Branch Model Policy/Guidance On "Limited Personal Use" Of Government Office Equipment Including Information Technology*," May 19, 1999

National Archives and Records Administration (NARA), General Records Schedule 12, Transmittal No. 8, Communications Records, §4 Telephone Use (Call Detail) Records, April 2010

Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, *Security Requirements for Cryptographic Modules (includes change notices as of December 3, 2002),*

Federal Information Security Management Act of 2002, 44 U.S.C. §3541, et seq. (2013)

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009

NIST SP 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, June 2010

NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, February 2007

NIST SP 800-121 Revision 1, *Guide to Bluetooth Security*, June 2012

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010

NIST SP 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013

NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, February 2012

Office of the Director of National Intelligence, U.S. Office of the National Counterintelligence Executive, *Tips from the National Counterintelligence Executive: Traveling Overseas with Mobile Phones, Laptops, PDAs, and Other Electronic Devices*

Office of Management and Budget (OMB) Circular No. A-11, *Preparation, Submission and Execution of Budget*, revised August 3, 2012

OMB Circular A-130, *Memorandum for Heads of Executive Departments and Agencies: Management of Federal Information Resources*, November 28, 2000

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Use of Government Property, 5 C.F.R. § 2635.704 (2012)