

DATE: January 22, 2014
TO: DIRECTIVES POINTS OF CONTACT
FROM: KEVIN T. HAGERTY, DIRECTOR
OFFICE OF INFORMATION RESOURCES
SUBJECT: Draft DOE O 203.2, *Mobile Technology Management*

The draft directive has been posted on RevCom for review and comment. The Order establishes requirements, assigns responsibilities, and provides guidance for federal mobile technology management and employee use of mobile devices within DOE.

INSTRUCTIONS

Headquarters DPCs have until **February 21, 2014**, to submit to the OPI consolidated comments received from subject matter experts and/or field DPCs using the Department's RevCom system (<https://www.directives.doe.gov/login.jsp>).

HQ DPCs

- may set separate deadlines for field offices using the RevCom "Version" link.
- must obtain approval from their secretarial officers or designees before submitting official organization comments.

Extensions to the commenting period will be granted only with the permission of the office of primary interest and only for the requesting organization.

Comments:

Please identify comments as "Major" or "Suggested." Major comments should be identified as addressing issues serious enough to preclude or significantly hamper the Department's ability to—

- accomplish policy objectives and missions,
- comply with applicable laws, rules, and regulations, or
- fulfill contractual obligations and formal commitments.

The first issue for consideration is whether this directive should apply to your organization. If it should not apply, enter that information with justification in the "Overall Comments."

OPI: The office of primary interest must respond to all comments submitted by Headquarters DPCs.

Please address questions on the content of the draft directive to Helen McBride(IM-22) at 202-586-7549; helen.mcbride@hq.doe.gov.

Questions on the directives program should be directed to Camille Beben (MA-90) at 202-586-4014; camille.beben@hq.doe.gov.

SUBJECT: MOBILE TECHNOLOGY MANAGEMENT

1. PURPOSE. To establish requirements, assign responsibilities, and provide guidance for federal mobile technology management and employee use of mobile devices within the Department of Energy (DOE) including the National Nuclear Security Administration (NNSA). For the purposes of this directive mobile devices includes both government furnished and personally-owned devices. Employees have the privilege of using personal mobile devices in accordance with operational use and release agreements signed by the employee.
2. CANCELLATION. None.
3. APPLICABILITY.
 - a. Departmental Applicability. Except for the equivalencies/exemptions in paragraph 3.c, this directive applies to all Departmental elements using government furnished or personally-owned mobile devices for accessing the DOE environment.
 - (1) The Administrator of the NNSA must assure that NNSA employees comply with their responsibilities under this directive. Nothing in this directive will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.
 - (2) The Administrator of the Bonneville Power Administration will assure that its employees comply with their respective responsibilities under this directive.
 - b. Site/Facility Management Contractors. This Order does not contain a Contractor Requirements Document. However, contractors are to ensure the use of mobile devices within their environment is appropriately addressed by their site Risk Management Approach (RMA) and consistent with the applicable Senior DOE Management RMA implementation in accordance with DOE O 205.1B, DOE Cyber Security Program, as currently amended.
 - c. Equivalencies/Exemptions.
 - (1) Requests for equivalencies and exemptions from paragraph 4 of this directive must follow the process outlined in paragraph 6.a.(3)(c) of DOE O 251.1C, Departmental Directives Program, as currently amended.

- (2) In accordance with the responsibilities and authorities assigned by Executive Order 12344, codified at 50 USC sections 2406 and 2511 and to ensure consistency through the joint Navy/DOE Naval Nuclear Propulsion Program, the Deputy Administrator for Naval Reactors (Director) will implement and oversee requirements and practices pertaining to this Directive for activities under the Director's cognizance, as deemed appropriate.

4. REQUIREMENTS.

- a. DOE offices will establish signed user agreements with individuals prior to the use of mobile technology within the DOE environment to perform official duties that address:

- (1) Safe use of mobile technology in accordance with DOE O 450.2, Integrated Safety Management, as currently amended.
- (2) Appropriate use of mobile technology in accordance with DOE O 203.1, Limited Personal Use of Government Office Equipment Including Information Technology, as currently amended.
- (3) Procedures for lost, stolen, or damaged DOE provided mobile devices in accordance with DOE O 580.1A, DOE Personal Property Management Program, as currently amended.
- (4) Timely reporting of loss of mobile devices containing Departmental data consistent with DOE O 205.1B, DOE Cyber Security Program, as currently amended.
- (5) Reimbursement guidance and procedures for the use of personally-owned mobile devices to perform official duties.

A recommended User Agreement document is provided in Appendix A.

- b. DOE offices that manage DOE IT assets and infrastructure must document and implement appropriate mobile device management procedures and oversight processes that address:

- (1) Use and/or prohibition of mobile devices for foreign travel.
- (2) Identity verification and authentication requirements for access to DOE data and systems via mobile devices.
- (3) Mobile device management (MDM) solutions for device monitoring and control for devices that store sensitive DOE information.
- (4) Encryption and sanitization requirements for mobile devices that are used for storing sensitive DOE information.

- (5) Patch management and configuration management procedures for mobile devices that store sensitive DOE information.
 - (6) Continuous monitoring procedures to detect compromise of mobile devices that store sensitive DOE information.
 - (7) Mobile device incident notification and reporting requirements.
 - (8) Mobile device inventory and reporting processes consistent with DOE O 580.1A, DOE Personal Property Management Program, as currently amended.
 - (9) Mobile device service termination processes.
- c. DOE offices shall train employees on processes and procedures relevant to using mobile devices within the DOE environment.
 - d. Consistent with DOE O 243.1B, Records Management Program, as currently amended, all devices that access DOE/NNSA Network resources and store Departmental records or data, may be subject to record retrieval for business purposes. It may be necessary for DOE offices to physically collect mobile devices in support of record retrieval if records have not been captured in another way.
 - e. DOE offices are prohibited from providing stipends for the use of personally-owned mobile devices for government work.
 - f. Mobile device owners use their personal devices at their own risk. DOE assumes no financial or legal liability for loss or damage of a personally-owned mobile device used for official duties.
 - g. DOE offices must leverage a technology solution that enables the enforcement of IT policies; revocation of access to DOE data and IT assets at any time; capability to wipe DOE records and data stored on devices (up to and including wiping a complete device in cases of classified spillage); and monitoring usage of mobile devices while actively accessing DOE/NNSA Network resources.
 - h. No classified material may be stored on mobile devices at any time. Inadvertent classified spillage to a personal mobile device that cannot be remediated by approved sanitation processes may result in destruction of the personal device without compensation to the owner. A recommended Acknowledgement of Spillage Procedures document is provided in Appendix B.
 - i. No DOE Personally Identifiable Information (PII) may be stored on personal mobile devices unless encrypted consistent with Federal Information Processing Standards (FIPS) 140-2 standards. DOE offices should provide guidance consistent with DOE O 206.1, DOE Energy Privacy Program, as currently amended.

- j. Personal mobile devices must leverage a technology solution that isolates the device from DOE data and DOE IT assets in such a manner that protects the confidentiality, integrity and availability of DOE data and controls the risk the personal device will compromise DOE IT assets. For example:
 - (1) A virtualization strategy that provides remote access to computing resources through a Virtual Desktop Infrastructure or legacy thin/zero client solution and does not permanently store DOE data on the device.
 - (2) A FIPS 140-2 validated encrypted containerization strategy that can be centrally monitored and configured and provides remote container-wiping capabilities.
 - (3) Another technical solution that encrypts and controls access to DOE/NNSA Networks and DOE data stored on the device (including enforcement of DOE password policies), and provides the capability to remotely wipe the DOE data from the device.
 - k. DOE offices are only required to provide technical assistance for issues directly related to software installed by DOE on a personally-owned mobile device.
 - l. Use of mobile devices does not negate the responsibility of programs to meet Federal and DOE requirements for managing and protecting information at rest and in transit. DOE offices must ensure that they follow their program policies and procedures for protecting data in transit and at rest as well as Federal and DOE policies and procedures.
5. RESPONSIBILITIES.
- a. Chief Information Officer (CIO).
 - (1) Establish and maintain Departmental policy related to use of mobile devices in the DOE environment. Annually review and revise policy as necessary to reflect advancements in technology and emerging security issues associated with the use of mobile devices.
 - (2) Establish enterprise mobile device contracts based on approved standards that allow for bulk procurements and volume savings by leveraging appropriate contract vehicles.
 - (3) Retain overall accountability for mobile device use within the DOE Enterprise Information Technology Services environment.
 - b. Chief Information Security Officer.
 - (1) Serve as the subject matter expert point of contact for the CIO for matters related to mobile technology security.

- (2) Provide advice and assistance, as necessary, to Program Secretarial Officers with regards to secure implementation of mobile technology.
- (3) Prepare Departmental mobile technology security implementation guidance as needed.
- (4) Report the DOE security posture implementation on behalf of the Department based on program reports and independent reviews of Program Office mobile technology implementation throughout the Department.

c. Program Secretarial Officers.

- (1) Retain overall accountability for mobile device use by their organization within the DOE IT environment.
- (2) Ensure applicable mobile device management procedures are implemented in a manner that cost-effectively reduces risks to an acceptable level while supporting mission requirements.
- (3) Ensure employees are appropriately trained and user agreements are signed prior to assigning a government furnished mobile device or approving use of a personal mobile device for accessing DOE information resources.
- (4) Monitor and report on the effectiveness of mobile device management procedures.

d. Federal Employees.

- (1) Use government furnished and/or personal mobile devices consistent with the requirements of this Order and applicable user agreements.
- (2) Complete mobile device training as required by organization mobile device procedures.
- (3) Read, understand, and sign appropriate user agreement forms. Consult supervisors or other appropriate persons if they have any questions related to the content or expectations of the user agreement.
- (4) Report all identified or suspected incidents occurring during use of a mobile device for official duties or involving DOE information resources.
- (5) Consult supervisors or other appropriate persons if they have any questions concerning this Order or related matters.

6. REFERENCES.

- a. OFFICE OF MANAGEMENT AND BUDGET (OMB) CIRCULARS. Located at http://www.whitehouse.gov/omb/circulars_default/
 - (1) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Revised November 2000
- b. OMB MEMORANDA PERTAINING TO MOBILE DEVICE MANAGEMENT AND USE. Located at http://www.whitehouse.gov/omb/memoranda_default/
 - (1) OMB Memorandum M-03-22 Guidance for implementing the Privacy Provisions of the E-Government Act of 2002
 - (2) OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, May 2006
 - (3) OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 2006
 - (4) OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, July 2006
 - (5) OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 2007
- c. DOE ORDERS, MANUALS, NOTICES, AND GUIDELINES. Located at <https://www.directives.doe.gov/directives>
 - (1) DOE O 203.1, Limited Personal Use of Government Office Equipment Including Information Technology, as currently amended
 - (2) DOE O 205.1B, DOE Cyber Security Program, as currently amended
 - (3) DOE O 206.1, DOE Privacy Program, as currently amended
 - (4) DOE O 251.1C, Departmental Directives Program, as currently amended
 - (5) DOE O 314.1, DOE-FLEX: DOE's Telework Program, as currently amended
 - (6) DOE O 450.2, Integrated Safety Management, as currently amended
 - (7) DOE O 473.3, Protection Programs Operations, as currently amended
 - (8) DOE O 471.6, Information Security, as currently amended
 - (9) DOE O 580.1A, DOE Personal Property Management Program, as currently amended

d. OTHER.

- (1) E-Government Act (Public Law 107-347), Title III - Federal Information Security Management Act, December 2002
- (2) The Privacy Act of 1974, 5 U.S.C. §552a
- (3) 5 CFR, Administrative Personnel, Parts 73 1 and 752 I. US Code, Title 18, Crimes and Criminal Procedures
- (4) 5 CFR 2635, Standards of Ethical Conduct for Employees of the Executive Branch OMB, Personal Use Policies and File Sharing Technology, dated 9-8-04
- (5) FIPS Publication 140-2, Security Requirements for Cryptographic Modules, February 2004
- (6) FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- (7) FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- (8) NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
- (9) NIST Special Publication 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy, September 2009
- (10) NIST Special Publication 800-46 Revision 1, Guide to Enterprise Telework and Remote Access Security, June 2009
- (11) NIST Special Publication 800-53 Revision 4, Recommended Security Controls for Federal Information Systems and Organizations, 2009
- (12) NIST Special Publication 800-53A Revision 1, Guide for Assessing the Security Controls in Federal Information Systems and Organizations, June 2010
- (13) NIST Special Publication 800-57r3, parts 1-3, Recommendation for Key Management
- (14) NIST Special Publication 800-61 Revision 1, Computer Security Incident Handling Guide, March 2008
- (15) NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling, April 2010

- (16) NIST Special Publication 800-88, Guidelines for Media Sanitization, September 2006
- (17) NIST Special Publication 800-92, Guide to Computer Security Log Management, September 2006
- (18) NIST Special Publication 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007
- (19) NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices, November 2007
- (20) NIST Special Publication 800-164; Guidelines on Hardware- Rooted Security in Mobile Devices, October 2012
- (21) NIST Special Publication 800-114, User's Guide to Securing External Devices for Telework and Remote Access, November 2007
- (22) NIST Special Publication 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011
- (23) Committee on National Security Systems Instruction 1001, National Instruction on Classified Information Spillage, February 2008
- (24) DOE HQ Controlled Articles Policy Rational, dated 8-26-10
- (25) DOE Bring Your Own Device Toolkit, dated 9-28-12
- (26) DOE Cloud Computing Toolkit, dated 9-28-12
- (27) DOE Mobility Toolkit, dated 9-28-12

7. DEFINITIONS.

- a. Acceptable Use. The ethical and allowable use of mobile computing devices at DOE. These acceptable use rules are in place to protect customers, business partners, and employees of DOE. Insecure practices and malicious acts expose DOE, 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 DOE. In addition, security breaches damage the DOE's reputation and could result in loss of services.
- b. Containerization. Refers to a process of containment by creating a separate, protected workspace from personal data on a mobile device in an effort to secure corporate data, protect against malware, and prevent unauthorized access via security policies.

- c. DOE/NNSA Network. Connection or access to DOE data or information that is located behind the DOE firewall and requires a DOE/NNSA Network logon to access.
- d. Electronically Stored Information. 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. Electronically stored information includes metadata.
- e. Personal Use. An activity conducted for purposes other than accomplishing official or otherwise authorized activity.
- f. Mobile Device. Hardware and associated software and services capable of transmitting, receiving, processing, or storing information across a wireless medium. Examples include but are not limited to mobile phones, smart phones, tablet computers, laptops, mobile Wi-Fi hotspots, mobile printers, mobile point-of-sale devices, and any other wireless device capable of transmitting, receiving, processing, or storing information, as well as associated software and services.
- g. Mobile Device Management (MDM). 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, and Personal Digital Assistants. 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.
- h. 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.
- i. Risk Management Approach (RMA). Analysis of threats/risks; risk-based decisions considering security, cost and mission effectiveness; and implementation consistent with guidelines from the National Institute of Standards and Technology (NIST) and Committee on National Security Systems cyber requirements, processes and protections.
- j. Personally Identifiable Information (PII). Any information collected or maintained by the Department about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment

history, and information that can be used to distinguish or trace an individual's identity, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual.

- k. Sensitive DOE Information. For the purposes of this document, sensitive DOE information includes PII, Privacy Act, Procurement, Financial, Unclassified Control Nuclear Information, proprietary and Official Use Only.
- l. Virtual Desktop Infrastructure. software technology that separates the desktop environment and associated application software from the physical client device that is used to access it.

Acronyms used in this Order are defined in Appendix C.

- 8. CONTACT. Questions concerning this Order should be directed to the Office of the CIO at (202) 586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

NAME

Deputy Secretary

Logo
inserted
here after
approval

USER AGREEMENT

PRIVACY ACT STATEMENT		
<p><i>AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131. - Identifies the user of this device on DOE/NNSA Networks as receiving usage and security awareness training governing use of the Networks and agreeing to use the Networks in accordance with security and wireless policies. The information is used for identification purposes and to verify compliance with DOE requirements regarding accountability of information processing systems, and provides emergency contact information on the user in the event that the user's access to the Networks becomes compromised, or requires a reconfiguration due to security policy changes.</i></p>		
PART I – User Information		
1. Last Name	2. First Name	3. Federal or Contractor
4. ORG	5. Location	6. Room Number
7. Primary Telephone	8. Alternate Telephone	9. Sponsor
10. Email Address		
PART II – User-Owned Devices Accessing DOE Resources		
Brand	Model	Serial #
PART III - Acceptable Use		
<p><i>[This section should be tailored to the individual processes and procedures of the cognizant Program Office.]</i> By signing this document, you acknowledge and consent to the following when you use the above mobile device(s) to access DOE/NNSA Networks:</p> <p>Use of the above mobile device(s) for work purposes is in strict compliance with the applicable designated Integrated Safety Management System established per DOE O 450.2, Integrated Safety Management, as currently amended, by the responsible DOE organization.</p> <p>Use of the above mobile device(s) does not result in the release of DOE information to unauthorized persons.</p> <p>All DOE data processed or stored on the above mobile device(s) may be audited, intercepted, recorded, read, copied, or captured and disclosed by authorized personnel. There is no right to privacy on:</p> <ul style="list-style-type: none"> • Any government information system, network or other government furnished device, or • Personally-owned mobile devices while being used to perform official duties. <p>This applies regardless of whether the access or use of an information system or device includes the display of a Notice and Consent Banner ('banner'). When a banner is used, the banner functions to remind the user of the</p>		

conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

DOE/NNSA IT Support or Cyber Security personnel may intercept and monitor communications and disclose any potential evidence of crime related to DOE IT assets and data found on above mobile device(s) to appropriate authorities for purposes including, but not limited to, communications security monitoring, network operations and defense, personnel misconduct, law enforcement, and counterintelligence investigations.

Users will update their devices with recommended software updates provided by the Department or the manufacturer of their device.

Users must follow security policies that govern the use of this connection and associated systems [*organizational specific guidance should be defined*]

Users are accountable at all times for the whereabouts and the security of their personal device(s), associated removable storage media and the DOE/NNSA data that may be retained within the device.

Users must protect the storage and transmittal of the following categories of sensitive information: Personally Identifiable Information, Privacy Act, Procurement, Financial, Unclassified Control Nuclear Information, proprietary and Official Use Only.

The above mobile device(s) must be installed with the DOE/NNSA authorized virtualization or containerization solution in order to securely process DOE/NNSA data. The device configuration must be approved by the system Authorizing Official.

Users must complete security awareness training annually and mobile technology training as required while using personal device(s) for accessing DOE/NNSA data and Networks. [*organizational specific training requirements should be provided*]

Users will report lost, stolen, or damaged government furnished mobile device(s) above consistent with DOE O 580.1A, DOE Personal Property Management Program, as currently amended. [*organizational specific reporting processes should be provided*]

Users will report loss of both government furnished and personally-owned mobile device(s) above that contain Departmental data consistent with DOE O 205.1B, DOE Cyber Security Program, as currently amended. [*organizational specific reporting processes should be provided*]

Users of personally-owned mobile device(s) above will be reimbursed for expenses incurred for the performance of official duties on the device upon submission of appropriate documentation of the expense. [*organizational specific reimbursement processes should be provided*]

By signing this user agreement, I am acknowledging that I accept and will abide by all the terms and conditions described above.

FOR REPORTING INCIDENTS OR TO ASK NETWORK QUESTIONS, CONTACT: [*organizational specific points of contact should be provided*]

User Name Printed	
User Signature & Date	

ACKNOWLEDGEMENT OF SPILLAGE PROCEDURES ON MOBILE DEVICES

As a condition for the privilege of using a personally-owned mobile device to perform official duties and access DOE/NNSA Networks, I, _____, understand and acknowledge that:

- a. If I own a device on which there is intentional or unintentional DOE data spillage, my personal device and data are forfeit. DOE has the right to sanitize/destroy my personal data and device in accordance with NSA sanitization procedures.
- b. If there is accidental or unintentional spillage on a device that I own, the organization will make every effort to conserve my personal data and device during all phases of data spillage remediation. If DOE is unable to successfully wipe my personal device of DOE information, my personal device may have to be destroyed.
- c. In the event that my device must be destroyed, DOE will not compensate me for the device or the personal data located on the device.

User Name Signed: _____

User Name Printed: _____

Date: ____/____/____

ACRONYMS

ACRONYMS. The acronyms listed in the following table are for terms used in the DOE O 203.2 Mobile Technology Management, as currently amended, including the appendices.

Acronym	Definition
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
DOE	Department of Energy
FIPS	Federal Information Processing Standards
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RMA	Risk Management Approach