

# Defense Logistics Agency INSTRUCTION

DLAI 8130.01 Effective September 27, 2013

J6

SUBJECT: Mobile Device Management

**REFERENCES:** Refer to Enclosure 1.

1. <u>PURPOSE</u>. This instruction:

a. Establishes the policy and procedures associated with the issuance and management of Mobile Devices.

b. Mobile technology is growing at an exponential rate. Devices are becoming smaller, faster and are proliferating throughout DOD and DLA. We now have handheld devices that can store and process amounts of information that was previously limited to desktops and laptops. These new devices are costly and are also a target of our adversaries and must be properly controlled. This instruction will ensure that all users of this technology understand the criticality of these devices and why they must be strictly controlled.

c. This policy excludes laptop computers.

2. <u>APPLICABILITY</u>. This instruction applies to DLA employees and contractor staff.

#### 3. **DEFINITIONS**.

a. Mobile Device: A wireless-enabled portable device (cellular phone, Blackberry, Personal Digital Assistant, iPad or tablet PC) that is owned, maintained, or supported by DLA.

b. Sensitive Information: The loss, misuse, unauthorized access or modification of which, could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act", but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of National Defense or Foreign Policy. (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987").

## 4. <u>POLICY</u>. It is DLA policy that:

a. All DLA employees and contractors that have been entrusted with the use of a mobile device must maintain positive control of that device at all times.

b. Each user issued a Mobile Device must sign a Mobile Device user agreement, will have a current, signed, DLA Rules of Behavior on file with their local Information Assurance or Network Services Branch, and will have a signed DLA Form 1813 (Request and Approval for off-Site Use of Government Information Technology Equipment) in their possession.

c. Mobile Devices may be taken overseas while on official business provided written approval is received from the trip authorizing official within each Primary Level Field Activity (PLFA) or J-code.

#### 5. <u>RESPONSIBILITIES</u>.

a. DLA Chief Technology Officer (CTO), under the authority, direction, and control of the Director, DLA Information Operations, is responsible for:

(1) The development and enforcement of mobile device strategy for the agency.

(2) Approval of different types of mobile devices for use.

b. DLA Information Operations (J64) is responsible for:

(1) The annual review and content of this Instruction.

(2) Ensuring compliance with DOD, DISA and DLA Instructions.

(3) Assessment and testing of emerging Mobile Device technologies.

c. J6 Lead for Network and Telecommunications Services is responsible for:

(1) Ensuring that Mobile Devices are only issued to those employees who justify and demonstrate the need for a Mobile Device in the performance of their daily duties.

(2) Complying with this and all other DOD, DISA and DLA instructions governing Mobile IT device maintenance and usage. Ensuring all Mobile Devices in use at their PLFA/Site are properly inventoried, tracked and that all required patching, software updates and compliance with any applicable Security Technical Instruction Guidelines (STIGs).

d. Employees are responsible for:

- (1) Complying with the provisions of this instruction.
- (2) Maintaining oversight of their assigned equipment.
- (3) Using the mobile device assigned to them for official use only.
- (4) Signing and adhering to the DLA Mobile Device user agreement.

# 6. <u>PROCEDURES</u>. Refer to Enclosure 2.

# 7. INFORMATION REQUIREMENTS. Not Applicable.

# 8. INTERNAL CONTROLS.

a. DLA Mobile Device Instruction. Each DLA user issued a mobile device is required to be familiar with the Mobile Device Instruction. The risk is that users may not understand the importance of maintaining strict control of mobile devices and how vital the need for accountability and auditability of our IT Equipment.

b. Mobile Device User Agreement. All users issued a mobile device must sign a user agreement, (see Enclosure 3), which includes a checklist of 15 actions that must be adhered to while operating the device. The risk is that for many users, mobile device usage has been common place for several years, however this may be their first experience with a government issued mobile device, which is subject to much more control and oversight than one procured for personal use.

c. Procedures. Refer to Enclosure 2.

9. <u>RELEASABILITY</u>. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DLA Issuances Internet Website.

#### 10. EFFECTIVE DATE, This Instruction:

a. Is effective on September 27, 2013.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with DLAI 5025.01, DLA Issuance Program. If not, it will expire effective September 27, 2023 and be removed from the DLA Issuances Website.

PHYLLISA S. GOLDENBERG Director, DLA Strategic Plans and Policy

Enclosures(s) Enclosure 1 – References Enclosure 2 – Procedures Enclosure 3 – User Agreement

# ENCLOSURE 1

# **REFERENCES**

- (a) Information Assurance (IA) Rules of Behavior, March 2, 2010, (https://headquarters.dla.mil/DES/policy/i6404.htm).
- (b) DoD Bluetooth Peripheral Device Security Requirements, July 16, 2010, (http://iase.disa.mil/stigs/downloads/pdf/DoD\_bluetooth\_requirements\_spec\_20100716.pdf).
- (c) DoD Guidance on Protecting Personally Identifiable Information (PII), August 18, 2006, (http://iase.disa.mil/policy-guidance/pii-signed-memo-08182006.pdf).
- (d) DISA Wireless Security Technical Implementation Guide (STIG), Version 6 Release 5, October 28, 2011, (http://iase.disa.mil/stigs/net\_perimeter/wireless/wireless\_net.html).
- (e) DISA BlackBerry STIG, Version 1 Release 7, October 28, 2011, (http://iase.disa.mil/stigs/net\_perimeter/wireless/smartphone.html).
- (f) DLA Information Technology Solutions, March 2013, (https://eworkplace.dla.mil/sites/org/j6/Shared%20Documents/dla%20IT%20Solutions%20D ocument.pdf).
- (g) Department of the Army Memo, Nov 14, 2011, Subject: U.S. Army Guidance on Piloting of Commercial Mobile Devices (CMD).
  (http://ciog6.army.mil/LinkClick.aspx?fileticket=BCZaMlQ3PGM%3D&tabid=64)
- (h) Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG), April 23, 2007, (http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf).
- (i) DoD Wireless Smartphone Security Requirements Matrix, Version 3.5, January 21, 2011, (http://iase.disa.mil/stigs/downloads/pdf/u\_DoD\_smartphone\_email\_system\_security\_req\_m atrix\_v3r5\_20110121.pdf).
- (j) DISA Secure Mobile Environment Portable Electronic Device (SME PED) STIG, Version 2 Release 1, April 29, 2011,

(https://powhatan.iiie.disa.mil/stigs/downloads/zip/fouo\_sme\_ped\_v2r1\_stig\_20110429.zip).

- (k) DoD Instruction 8500.2, Information Assurance (IA) Implementation, February 6, 2003, (http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf).
- (1) DISA Draft General Mobile Device (Non-Enterprise Activated) STIG, Version 1, Release 3, April 26, 2013, (http://iase.disa.mil/stigs/net\_perimeter/wireless/smartphone.html).
- (m)DISA Android 2.2 (Dell) STIG, Version 1, Release 1, November 23 2011, (http://iase.disa.mil/stigs/net\_perimeter/wireless/smartphone.html).
- (n) DISA ISCG for Apple iOS 6 Technology Overview, Version 1, Release 1, January 4, 2013, (http://iase.disa.mil/stigs/net\_perimeter/wireless/smartphone.html).
- (o) Instant Messaging STIG, Version 1, Release 2, February 15, 2008, (http://iase.disa.mil/stigs/downloads/pdf/instant\_messaging\_stig\_v1r2.pdf).
- (p) DoD Instruction 6055.04, DoD Traffic Safety Program, January 23, 2013, (http://www.dtic.mil/whs/directives/corres/pdf/605504p.pdf).
- (q) DLA Flash Media Guidance, December 7, 2005, (https://eworkplace.dla.mil/sites/org3/des/Shared% 20Documents/DES-B/One% 20Book% 20Electronic% 20Library\_0\_/1.% 20One% 20Book% 20Chapters% 20and% 2

0Flowcharts/Policy%20Letters/letter120705%20Use%20of%20Flash%20Memory%20Devic es.pdf)

- (r) DoDM 5200.01-Vol. 1-4, DoD Information Security Program February 24, 2012
- (s) DoDI 5205.02E, DoD Operations Security (OPSEC) Program, June 20, 2012
- (t) DoDM 5205.02, DoD Operations Security (OPSEC) Program Manual, November 3, 2008
- (u) DLAI 6305, Operations Security (OPSEC), October 30, 2008, Modified May 27, 2011
- (v) DLAI 6304, Information Security Program, modified March 16, 2010

# ENCLOSURE 2

#### PROCEDURES

1. This enclosure provides a detailed list of procedures specifying how to properly use their device. The risk is that a user could introduce classified information onto unclassified media, or engage wireless or blue tooth settings within an area or zone not cleared for that type of connectivity.

2. Usage of DLA mobile devices must conform to the following policies, which are broken down into topic areas: general usage, email and messaging, web browsing, security, applications, connections and peripherals, multimedia, and enterprise configuration management.

a. <u>General Usage</u> – The following policy tenets pertain to overall mobile device usage:

(1) Users shall not process classified information on mobile devices. In the event of classified information spillage on mobile devices, immediately contact the local Information Assurance Officer (IAO) or your supervisor.

(2) Users shall not transmit or receive sensitive information (e.g., For Official Use Only (FOUO), Privacy Act Information, or information on the critical information list) via email on a mobile device unless Public Key Infrastructure (PKI) is enabled. Emails containing sensitive information must be signed and encrypted.

(3) When PKI is enabled, users may use approved mobile devices to process limited amounts of sensitive information; users must delete the files as soon as they are no longer required.

(4) Storage of Personally Identifiable Information (PII) on mobile devices must abide by current regulations set forth in the Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII).

(5) Mobile devices are not allowed in any area where classified documents or information is stored, transmitted, or processed without written approval from the Designated Approval Authority (DAA) or DLA, Chief Information Officer, in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA) (DLA Intelligence Office).

(a) Without DAA approval, devices must be left outside of classified areas where classified information is discussed, possessed, or processed.

(b) Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA in consultation with the CSA CTTA. The

responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures.

(6) Use of DLA internet access, phone, messaging, and email services for non-official purposes is permitted only under the following circumstances:

(a) Usage does not adversely affect the employee's performance or accomplishment of the DLA or DoD mission, and usage does not reflect adversely on DLA, DoD, or the Federal Government.

(b) Usage will occur on breaks, lunch periods, and non-duty hours.

(c) Usage precludes any unnecessary costs or appearance of impropriety to the Federal Government. For more information, please reference the Information Assurance (IA) Rules of Behavior (ROB) referenced in Enclosure 1.

(d) For guidelines relating to the use of Social Media on mobile devices or other electronic equipment please reference the DLA Social Media Policy.

(7) Users shall sign a user agreement and comply with any necessary mobile device training requirements before a mobile device is issued.

(8) Mobile device users must complete annual training on device use and security.

(9) Users shall exercise caution when using DLA mobile devices and are prohibited from using Government-supplied electronic equipment for text messaging or other hand-held uses while driving unless the vehicle is safely parked or they are using a hands-free device, except for receiving or placing calls in performance of duties from tactical or emergency vehicles or other mission critical duties, to include law enforcement use of in-car mobile data terminals and other in-car electronic devices. Even with hands-free devices, use of mobile devices while driving is discouraged.

b. <u>Applications</u>. The following policy pertains to application installation, use, and removal on mobile devices:

(1) Access to public application repositories (e.g., public App Stores) shall be disabled.

(2) All applications shall be approved by the DAA and have a risk assessment completed prior to deployment.

(3) Approved applications will be listed in the DLA Information Technology Solutions document.

c. Email.

(1) If mobile device email signatures are used, the signature message shall not disclose that the email originated from a mobile device (e.g., "Sent From My BlackBerry Wireless Handheld").

(2) Only email solutions provided by the DLA standard device configuration are approved for use.

(3) Only DLA email accounts shall be configured on mobile device email clients.

(4) Users will only send DLA email that contains sensitive information when PKI (signing/encryption) is enabled.

d. Messaging.

(1) The messaging function will be disabled with the option to enable upon request and subsequent approval by the DAA for the accomplishment of official business.

(2) The DAA or CIO may pre-approve the messaging function for select user groups or certain business functions.

(3) Text messaging and other messaging services should be used when necessary, and will not contain classified or sensitive information.

(4) DoD/DLA approved and hosted enterprise messaging services are permitted on mobile devices.

(a) All instant messaging services must be hosted by a DoD site.

(b) Approved messaging services are listed in the Information Technology Solutions document.

(5) Picture and video messaging will be disabled with the option to enable upon request and subsequent approval by the DAA or CIO for the accomplishment of official business. For more information, see DLA Physical Security Manual and local policy for guidance on picture taking.

e. Connections

(1) Cellular Voice and/or Data. Mobile devices shall only connect to DLA-approved cellular carriers, as configured by DLA Site Administrators. Users shall not attempt to "unlock" or otherwise modify devices to change carriers.

(2) Bluetooth.

(a) Bluetooth shall be disabled and use is prohibited except for the following two use cases:

<u>1</u>. Use of a DAA tested and approved Bluetooth Common Access Card (CAC) reader (e.g., Bluetooth Smart Card Reader (SCR) with dongle, if required) is permitted.

<u>2</u>. Bluetooth for voice and audio transmissions (e.g., Bluetooth headset or handsfree device) is permitted only for mobile devices and headsets approved by the DoD and DAA. See a Systems Administrator or IAO to determine if the mobile device and headset is approved for voice/audio transmissions using Bluetooth.

(b) When configured for approved use, Bluetooth shall be disabled/turned off when not actively being used.

(3) Universal Serial Bus (USB).

(a) USB connections are authorized for tethering mobile devices (for the purpose of providing an Internet connection) to Government Furnished Equipment (GFE) desktops/laptops. USB connections to non-GFE machines are prohibited.

(b) Mobile devices are not permitted to be used as removable USB storage devices.

(4) Wi-Fi.

(a) Hotspot-capable mobile devices are not permitted to broadcast Wi-Fi signals as an access point (i.e. function as a router for a wireless network).

(b) Wi-Fi capable mobile devices are permitted to connect to public wireless hotspots (e.g., at hotels, coffee shops) when necessary.

(c) Wi-Fi capable mobile devices shall be configured to prompt users before connecting to wireless local area networks (WLANs). Automatically connecting to WLANs is not permitted.

(d) Wi-Fi capable mobile devices are permitted to connect to personally-owned and controlled home WLANs. When using this option, the following security settings are required:

 $\underline{1}$ . The wireless network shall be secured with Wi-Fi Protected Access 2 (WPA2) encryption.

2. Mobile devices shall not be set to automatically connect to Wi-Fi networks.

<u>3</u>. Wi-Fi radios shall be disabled unless actively being used.

<u>4</u>. Reference the Defense Information Systems Agency (DISA) Wireless Security Technical Implementation Guide (STIG) or device specific STIGs (e.g., BlackBerry) for additional information regarding connecting mobile devices to home WLANs.

(5) Connected Devices. Pursuant to reference (r), connection of mass storage devices (e.g., USB flash drives, external hard drives) to DLA provided mobile devices is not permitted, unless otherwise approved by the DAA or CIO. If this approval has been granted, storage devices must be encrypted and follow the DLA Removable Flash Media Policy.

#### f. Security Settings

(1) Security settings for mobile devices shall comply with the minimum standards outlined in the appropriate DISA STIG for that specific device.

(2) A DoD logon banner will be displayed at login on mobile devices.

(3) Passwords/Logins.

(a) Users must be properly authenticated to use mobile devices. This can be accomplished by various methods, such as passwords/pass-codes and a CAC plus a PIN.

(b) Different devices have different authentication requirements and limitations. Specific information relating to authentication credentials (e.g. password length and complexity) will be enforced via a mobile device management solution (e.g. RIM BES). Users will not be able to change these settings.

(c) Regular passwords changes will be enforced per policy configuration via a mobile device management solution.

(d) After a preset number of incorrect authentication attempts, the information contained on the device will be automatically erased. The number of incorrect attempts allowed before a wipe will be enforced per policy configuration.

(e) Devices will be configured to automatically lock after a preset amount (time) of inactivity. Authentication credentials (e.g. password, CAC plus PIN) will be required to unlock the device when this occurs. This period of inactivity is governed by policy configuration, and may also vary by device.

(f) These policies will be enforced at an enterprise level.

(4) Physical Security. The following policies pertain to the physical security of mobile devices.

(a) DLA personnel shall maintain physical control of mobile devices at all times. Devices shall not be left unlocked and/or unattended in public places.

(b) Mobile devices shall not be loaned or otherwise given to any person other than whom the device is assigned to.

(c) In the event that a mobile device is lost or stolen, personnel shall immediately notify the site IAO/ IAM and their supervisor.

(d) DLA personnel shall be cognizant of the physical environment where they are using their mobile devices to access sensitive information or have sensitive voice conversations. For example, personnel shall take care to make sure unauthorized persons cannot see the device's screen when sensitive information is being accessed.

(e) Users shall not take DLA mobile devices on international travel unless specifically authorized by their PLFA/Site Commander or Director. Any devices that have returned from international travel shall be inspected for evidence of hardware and/or software tampering by the applicable DLA Information Operations Office System Administrator.

(5) Firewalls/Antivirus

(a) Firewall and antivirus solutions are enabled by the System Administrator and will be managed by the System Administrator.

(b) Mobile device antivirus software shall automatically remain up-to-date through infrastructure maintained by DLA/DISA.

(c) Users shall not attempt to disable or otherwise change firewall and antivirus configuration settings.

(6) Encryption. The following policy procedures pertain to data encryption on mobile devices:

(a) All mobile devices used to process DLA information shall employ data-at-rest encryption to protect DLA information stored on the device.

(b) All mobile devices used to process DLA information shall employ data-in-transit encryption to protect DLA sensitive information as it is transmitted/received by the device.

(c) DLA sensitive information shall never be transmitted/received via an unencrypted connection.

(d) All encryption solutions shall be Federal Information Processing Standard (FIPS) 140-2 validated.

g. <u>Web Browsing</u>. Only browsers provided by the DLA standard device configuration are approved for use. Approved Devices. The following policy procedures pertain to mobile devices approved for accessing DLA email and systems/network:

(1) Only DAA approved devices, mobile devices, operating systems, applications, network/PC connection methods, and wireless services shall be used.

(2) Approved devices are listed in the DLA Information Technology Solutions document, reference (f). When approved by the DLA Chief Technology Officer, additional devices are allowed in limited pilot programs when in the Defense Risk Assessment (DRA) or Interim Authority to Operate approval has been provided.

(3) Users shall not attempt to circumvent built in device security ("hack", "jailbreak", or "root") as this compromises the security posture of the device. Device integrity will be enforced through an enterprise Mobile Device Management (MDM) solution and/or random audits of devices.

h. <u>Multimedia</u>. The following policy procedures pertain to the use and storage of multimedia (audio, video, pictures/photos, and streamed content) on mobile devices:

(1) The use of removable media such as Secure Digital (SD) cards is not permitted, unless otherwise approved by the DAA or CIO. If DAA/CIO approval has been granted, removable media must be encrypted and stored separately from the mobile device to prevent loss of media storage and device together, and removable media must be bound to only one mobile device.

(2) The storage of personal music, pictures, and videos on mobile devices is prohibited.

(3) Streaming audio/video on mobile devices will follow Information Assurance (IA) Rules of Behavior (ROB) (Referenced in Enclosure 1).

(4) Use of mobile device digital cameras (still and video) is prohibited unless specifically approved by the DAA or CIO for specific official business.

(5) Screen capture functionality on mobile devices shall be disabled.

i. <u>Enterprise Management</u>. The following policy procedures pertain to management of hardware, applications, and firmware at an enterprise level:

(1) Where possible, components of this policy will be enforced by standard device configurations at an enterprise level.

(2) Configuration of mobile devices will be handled by an enterprise Mobile Device Management (MDM) solution (e.g., BlackBerry Enterprise Server, Good Mobility Suite, etc.) and shall not be changed by the user.

(3) The specific software image that will be installed on the mobile devices will be determined by the approved device, device OS and software versions as listed in the IT solutions document for mobility at the time of deployment. The device image could change as new versions of approved mobile applications and operating systems become available.

(4) Devices will be centrally managed by an enterprise MDM solution with the following capabilities:

- (a) Ability to remotely wipe devices.
- (b) Ability to set and enforce security configurations.
- (c) Audit logging.
- (d) Email redirection and routing.
- (e) Internet browser configuration.
- (f) Authentication.
- (g) Enforcement of data-in-transit and data-at-rest protection.
- (h) Software updates and patch management.

(5) Location services (e.g., Global Positioning System (GPS)) on mobile devices shall be disabled through enterprise MDM. Exceptions for specific applications shall be obtained through the DAA or Command Application Configuration Control Board (CCB).

# ENCLOSURE 3

# **USER AGREEMENT**

# **Mobile Device – User Agreement**

# **Equipment received**

Signing this user agreement constitutes your consent that the wireless device you have been issued is for **Official Government Use Only**, and that you agree to the receipt of the following items:

Mobile Device	Make/Model	MEID / Serial No	Wireless Carrier	Accessories

# **General Requirements**

[] User must immediately notify IAO/IAM and supervisor if his/her mobile device has been lost or stolen.

[] Do not connect DLA issued Mobile Device to non-Government furnished computer.

[] If prompted to perform software updates, deny the request and contact IAO/IAM.

[] Users will not install applications on the devices unless authorized by the DLA Designated Approving Authority (DAA) or Chief Information Officer.

[] Users will not take mobile devices overseas unless granted approval in writing from their PLFA/Site Commander or Director.

[] Users are required to read and acknowledge that they understand the requirements of the Mobile Device Policy.

# **Bluetooth Settings**

[] The Bluetooth settings must be set to off at all times except as allowed within Enclosure 2 topic e, Connections.

[] Bluetooth sharing of files is prohibited.

# **Mobile Device Wi-Fi Control**

[] The Wi-Fi radio must be disabled as the default setting and is enabled only when Wi-Fi connectivity is required.

# **Locations Services**

[] Location services must be turned off unless authorized for use for particular applications.

# **Classified Information**

[] Mobile devices must not be used in and around classified processing areas.

[] If a Data Spill occurs, immediately notify your IAO/IAM and your supervisor.

[] Wireless email devices will not to be used to send, receive, store, or process classified information.

[] Mobile Devices will not be connected to classified DoD networks or information systems.

[] Do not discuss sensitive or classified information on non-secure (devices not FIPS 140-2 certified or NSA Type -1 certified for voice) Mobile Devices.

# Please sign this agreement and provide the information requested, below.

USER INFORMATION			
NAME (Include rank - if military):	ORGANIZATION:		
USER WORK ADDRESS:	RANK (GS or military):		
	WORK STATUS (Military, government employee, or contractor):		
JOB SERIES:			
SIGNATURE OF USER	DATE SIGNED (YYYYMMDD)		