



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, US ARMY GARRISON, PRESIDIO OF MONTEREY
1759 LEWIS ROAD, SUITE 210
MONTEREY, CA 93944-3223

ARR 0 6 2022

AMIM-PMG-IMO

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Command Policy #28, Wireless Devices

1. References:

- a. AR 25-1, Army Information Technology Management, 15 July, 2019
- b. AR 25-2, Army Information Assurance (RAR), 4 April, 2019
- c. AR 25-13, Army Telecommunications and Unified Capabilities, 11 May 2017
- d. AR 735-5, Property Accountability Policies, 9 November 2016
- e. DOD 5500.7-R, Joint Ethics Regulation, 17 November 2011
- f. AD 2019-23 Memo, Subject: Allocation of Wireless Portable Electronic Devices, 1 August 2019
- g. DA PAM 25-1-1, Army Information Technology Implementation instructions, 15 July 2019

2. Purpose: Establish Command Policy for the acquisition and use of wireless devices to include: cellular telephones, Wi-Fi HotSpots, personal data assistants (PDA's) and Smart Phones (Apple, Android) for the United States Army Garrison Presidio of Monterey (USAG POM).

3. Applicability: This policy applies to all USAG POM personnel. This policy supersedes all previous versions.

4. Proponent: The Information Management Officer (IMO) is responsible for managing and administering wireless device authorizations, monitoring and validating authorized usage, and authorizing wireless carrier invoice payments. POC: Information Management Officer, (831) 242-6835/DSN 768-6835

5. Policy: Wireless devices can be provided only as required to meet the Garrison mission and duties assigned. The devices enhance efficiency and effectiveness of

AMIM-PMG-IMO

SUBJECT: Command Policy #28, Wireless Devices

Garrison mission operations and provide rapid communications where needed. Because of the high cost, close management and control over their use is required. Garrison Directors, Management and Support office Chiefs, or Division Chiefs must validate, approve and monitor wireless device requirements for their subordinates.

6. Action:

a. Directors, Management and Support Office Chiefs and Division Chiefs will:

(1) Approve wireless devices and service plans for their employees, and submit a signed Authorization Request for Wireless Device (Appendix A) to the IMO for action. The form is available on the SharePoint Library under PoM Forms:

https://army.deps.mil/army/cmds/imcom_usag9/presidio/Library/Forms/AllItems.aspx

(2) Disapprove requests for wireless devices if the requested instrument is to be used for any of the following purposes:

(a) Used solely for the user's convenience or personal use without operational necessity, or used to replace their personally owned wireless device.

(b) Used in lieu of official available fixed telecommunications systems (e.g. DSN, LAN lines, etc.).

(3) Oversee the use of wireless devices within their organizations and ensure appropriate action is taken when cases of unauthorized use are suspected or identified.

(4) Assist the IMO in performing quarterly audits of wireless devices assigned to their Directorate to ensure they are accounted for and in the possession of the individual to whom the device is assigned.

b. The Garrison IMO will:

(1) Procure and issue wireless devices.

(2) Maintain a database, to include:

(a) Name, organization and duty position of the employee issued a wireless device

(b) Assigned phone number and type of wireless device issued

(c) Date of issuance and whether it is permanent or temporary

(d) Wireless service plan provided, along with the plan cost

AMIM-PMG-IMO

SUBJECT: Command Policy #28, Wireless Devices

(e) Date and condition of the wireless device when returned, disconnected, suspended, reassigned or upgraded.

(3) Review itemized wireless device bills for unofficial or improper use. When necessary, require organizations/directorates to justify or reimburse expenses for unofficial calls (the IMO will coordinate any required collections through Garrison Resource Management).

(4) Compile statistics on wireless device use and prepare a monthly report to the DGC. These statistics will be used to revalidate wireless devices and determine service plan changes.

(5) Perform quarterly audits of wireless devices to ensure they are:

(a) Accounted for and in the possession of the individual to whom the device is assigned.

(b) In good working order.

(c) Returned to the IMO when no longer needed. (The user is required to e-sign their original AUP in the return device block on page 7, as wireless devices are considered to be durable property.

(6) Provide life cycle management and replace devices with an upgraded model (provided at no cost to the Government) in accordance with (IAW) the applicable service plan.

(7) Serve as the subject matter expert (SME) and primary command point of contact for all issues concerning wireless device use within POM.

c. Authorized Wireless Device Users will:

(1) Read and e-sign the following:

(a) PoM Acceptable Use Policy (AUP), acknowledging the user's understanding of the policy, including reimbursement to the Government for any unauthorized use.

(b) DMUC End User License Agreement (EULA), acknowledging the user's understanding of device and network security, device functionalities/capabilities, and accountability of Government mobile devices.

(2) Use the government wireless device IAW the principles of acceptable use for wired devices (ie: desktops, laptops, telephones, facsimile machines or other common office electronic devices).

(3) Be provided the minimum equipment and service plan required to perform official duties. This includes use while traveling on Government business for the purpose of notifying family members of any schedule or transportation changes and of safe arrivals and departures, use while TDY or working off-site for extended periods when use of LAN lines is not possible, use to enhance the professional skills and knowledge of Garrison employees, or to aid in the performance of duties.

7. Personal Use: It is unwarranted to require individuals authorized and required to carry a wireless device to also carry a personal device for routine communications. IAW references (a) and (f), wireless device use is permitted for brief communications of a personal nature for the purpose of checking on family, scheduling appointments (e.g. doctor, auto, home repair, etc.), brief Internet searches, e-mailing directions or sharing non-work related information, etc. Such personal communications are permitted as long as they:

a. Do not adversely affect the performance of official duties.

b. Are of reasonable duration (normally five minutes or less) and frequency (normally a few times a day), and are made during breaks, lunch periods or other off-duty periods.

c. Do not result in the user exceeding their authorized service plan. Users should consult the IMO to find out the details of the specific service plans for their wireless device.

8. Prohibited uses include:

a. Calls, e-mail or web searches that would reflect negatively on the Garrison and U.S. Army, such as sexually explicit and/or pornographic communications, images, or audio files, expressions of sexual or other forms of harassment, unofficial advertising, soliciting or selling intended for personal financial gain, or any form of gambling.

b. Activities inconsistent with DoD/Garrison policy or that violates other Army policies or laws such as: violating intellectual property and copyright law, supporting or promoting political agendas and/or candidates, or expressing subversive content incompatible with public service or in support of terrorist or subversive activities.

c. Actions that result in the theft of or abuse of wireless devices and/or services which cause unauthorized access, use, transfer or tampering with electronic accounts and files of others which result in the disruption, interference or loss of the work of others including, but are not limited to:

(1) Creating, downloading, storing, copying, transmitting or broadcasting chain letters.

AMIM-PMG-IMO

SUBJECT: Command Policy #28, Wireless Devices

(2) Sending "spam" or "letter-bomb" emails/texts designed to transmit repeatedly or interfere with the recipients' use of e-mail or texting features; or transmitting e-mails/text to large groups (entire organizations) instead of targeting the relevant audience, or disseminating large files over e-mail instead of using shared drives.

(3) Employing applications for personal use using: streaming data, audio, or video, malicious logic and virus development software tools and files, unlicensed software or games, Web altering tools/software, and other software that may cause harm to Government computers and telecommunications systems, or transmitting unsubstantiated virus warnings via e-mail/text from sources other than system administrators.

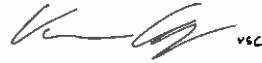
9. Cost Control: Users shall ensure costs are minimized and avoid additional usage charges.

a. Directory Assistance and transmission of pictures or images incur additional charges and should only be used when absolutely necessary to execute assigned duties and as authorized.

b. Users traveling outside of the United States on TDY, taking long personal vacations or any other circumstances in which they will not need or use their wireless plan for an extended period of time should contact the IMO to have their service plan temporarily suspended to avoid unnecessary charges.

c. Additional usage charges above the minimum service plan resulting from personal use are the responsibility of the user. Excessive or unauthorized personal use could result in the revocation of the wireless device authorization and/or disciplinary action.

Digitally signed by
CHHOEUNG.VARMAN.SO
K.1050078961
Date: 2022.04.06
13:52:22 -07'00'



2 Encls
Appendix A: Acceptable Use Policy
Appendix B: Wireless Authorization

VARMAN S. CHHOEUNG
COL, SF
Commanding

DISTRIBUTION: G



DEPARTMENT OF THE ARMY
UNITED STATES ARMY INSTALLATION MANAGEMENT COMMAND
HEADQUARTERS, US ARMY GARRISON, PRESIDIO OF MONTEREY
1759 LEWIS ROAD, SUITE 210
MONTEREY, CA 93944-3223

Acceptable Use Policy (AUP): Wireless Devices

1. References:

- a. AR 380-5, Department of the Army (DA) Information Security Program and this policy, 22 October 2019.
- b. AR 25-2 Army Information Assurance (RAR), 4 April 2019.
- c. DoD 5500.7-R, Joint Ethics Regulation, 17 November 2011.
- e. AUP for Defense Language Institute Foreign Language Center and Presidio of Monterey Installation Campus Area Network (ICAN) and Classified Campus Area Network (CCAN) 7 Jun 2016.

2. Purpose. The purpose of this policy is to outline the acceptable use of wireless cellular devices and satellite phones for the U.S. Army Garrison, Presidio of Monterey (POM). This policy applies to all Garrison employees requiring issuance of wireless devices.

3. Policy. By signing this document, the user acknowledges and consents that when using Department of Defense (DoD) cellular and satellite telephone devices:

- a. User is accessing cellular and satellite telephone device that is provided for U.S. Government authorized use only.

- b. User consents to the following conditions:

- (1) The provisions of reference (e) that apply to the ICAN or CCAN apply to all cellular and satellite telephone devices that interacts with the ICAN. A signed copy of reference (e) will be attached to this signed document for all users that connect to the ICAN or CCAN.

- (2) User may only use Government resources, to include Government owned wireless devices for official use and authorized purposes.

Acceptable Use Policy (AUP): Wireless Devices

4. **Access.** Access to cellular and satellite devices are for official use and authorized purposes as set forth in references below (para 5a thru 5e).

5. **Revocability.** Access to Army resources is a revocable privilege. Access may be revoked for any violation of the AUP or any action that puts the ICAN at risk. Cellular and satellite telephone devices will be re-instated only after the following conditions have been met:

a. The user involved has re-taken and completed the Information Assurance (IA) Awareness training.

b. The user involved has re-signed the general and the cellular and satellite telephone devices AUP.

c. The user's supervisor has requested re-instatement of cellular and/or satellite telephone devices.

6. **Personnel responsibility statement.** User agrees to the following security rules and requirements:

a. User will complete initial and annual Information Assurance (IA) Awareness training and participate in all training programs as required (including Personal Identifiable Information (PII); Data-At-Rest (DAR), Phishing, encryption, road warrior, physical security, acceptable use policies, malicious content and logic identification, and non-standard threats such as social engineering) before and after receiving cellular or satellite telephone devices.

b. User is responsible for any and all activity that occurs on the assigned wireless device. User is the only authorized user of this device. Users will not share Common Access Card (CAC) or reveal Personal Identification Number (PIN) with anyone. User will notify the POM Information Assurance Manager (IAM) immediately of any breaches of access.

c. Users will logon to the wireless device using a password and will follow password guidance as specified in the general AUP.

d. Users will ensure that any and all sensitive and PII is not emailed unless a digital signature and encryption is configured for that device.

e. User will not attempt to access or process data exceeding authorized Information Security classification level. User will not process or transmit classified information on the wireless device.

Acceptable Use Policy (AUP): Wireless Devices

f. User will secure government-owned wireless devices when not in use and not in their possession.

g. User will not alter, change, configure or use any hardware, operating systems or programs without prior written approval from the Information Management Officer.

h. User will not utilize Army or DoD provided wireless device for commercial/financial gain or illegal activities.

i. User understands that only a System Administrator or an authorized technician may perform hardware and software installations and maintenance. User is allowed to upgrade mobile devices to the most current software upgrade when directed by when directed by DoD Mobility Team.

j. User understands the wireless device will lock automatically after inactivity and will not disable this feature.

k. User will address any questions regarding acceptable use to the Garrison Information Management Officer, Mr. Carl Gunderson, Building 614, Ste 209, 831-242-6835, carl.l.gunderson2.civ@mail.mil.

l. In addition to the specific prohibitions outlined in AR 25-2, User understands that the following activities are not acceptable users of government equipment and are prohibited:

(1) The intentional introduction of a virus, worm or a Trojan horse on any wireless device.

(2) The intentional breaking into, damaging, defacing or destroying any wireless device belonging to another person, activity, agency or entity.

(3) Accessing pornography or obscene material without an official purpose.

(4) Accessing gambling related sites without an official purpose.

(5) Copying copyright-protected software, literature, music or video, except as authorized under the Fair Use Doctrine.

(6) Accessing hate speech or materials that ridicule or discriminate against others on the basis of race, creed, religion, color, gender, disability, national origin, or sexual orientation without an official purpose.

Acceptable Use Policy (AUP): Wireless Devices

(7) Political transmissions, including, but not limited to, transmissions that advocate the election of particular candidates for public office.

m. User understands that the following activities are considered acceptable uses of an Army Cellular device and are generally authorized at POM, provided the use is of reasonable duration and frequency and does not adversely affect the performance of official duties; involve commercial gain or the operation of a personal business enterprise; reflect adversely on POM, DA, DoD or create any significant additional cost to POM:

(1) During duty hours:

(a) Checking in with your spouse or minor children.

(b) Scheduling medical/dental appointments.

(c) Sending E-mails to build office morale by keeping employees informed of office activities.

(d) Browsing for professional information having relevance to your official duties.

(2) During lunch/non-duty hours:

(a) Arranging for appointments such as home/auto repairs.

(b) Brief visits/searches to acceptable Internet sites for personal use.

n. User will not store or transmit personnel medical data or privacy act material without proper encryption or other safeguards.

o. User will not use e-mail to:

(1) Create, download, store, copy, transmit, or broadcast chain letters.

(2) "Spam" to exploit list servers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.

(3) Broadcast unsubstantiated virus warnings or messages from sources other than approved NEC, DA, or DoD sources.

Acceptable Use Policy (AUP): Wireless Devices

(4) Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller specifically interested populations unless specifically approved and configured by the POM NEC.

(a) User will not use personal/commercial e-mail to conduct official government business.

(b) User will not forward official mail to non-official accounts or devices.

(c) User will not configure or download their personal email account to the government issued iPhone.

7. Apple iPhone Devices.

a. User will be held responsible for damage caused to a cellular/smartphone device or data through negligence or a willful act. Cost to replace the cellular or smartphone device will be the sole responsibility of the user. Note: the price for an out-of-cycle replacement (upgrade) will be the full retail price of the device offered by the wireless provider.

b. User is not authorized and will not use Bluetooth technology with iPhone devices except for the authorized CAC sled found on the Army approved two way wireless email device listing.

c. User will not operate a wireless device within 100 feet of any areas where classified information is electronically stored or processed.

d. User understands that all charges incurred in excess of the normal monthly service charge will be the responsibility of the iPhone user. Charges will be incurred for the following misuses of the device: exceeding allocated minutes per month, neglect or abusive damage to the device or accessory, or loss of the device.

e. User understands that the use of the Government issued iPhone device is **For Official Use Only**, and will not modify the settings of the device or software in any manner to facilitate the use of commercial e-mail systems.

8. SMS (Short Messaging Service) also known as "Text Messaging" on iPhone\Wireless devices create additional security concerns . User is aware of the following risks when utilizing the SMS (Text Messaging) service:

Acceptable Use Policy (AUP): Wireless Devices

a. Messages are not encrypted and copies are stored in memory on the phone and in the wireless carrier database. Sensitive information should not be sent via SMS/Text Messages/Multimedia Messaging Service (MMS).

b. Links to hacker web sites can be sent to a SMS/Text Message/MMS. If a user connects to the site address, malware could be downloaded on the phone.

c. Executable files (including malware) can be embedded in SMS/Text Message/MMS.

d. Photos sent via SMS/Text Messages/MMS can have links to hacker web sites embedded in the photo. When the photo is viewed, the phone will connect to web site of the embedded website.

e. Photos sent via SMS/Text Messages/MMS can have executable files (including malware) embedded in the photo. When the photo is viewed, the phone will execute the file.

9. Privacy Act Notice. The information below will be used to identify you and may be disclosed to law enforcement authorities for investigating or prosecuting violations. Disclosure of this information is voluntary; however, failure to disclose the information could result in denial of access to cellular and satellite telephone devices.

10. Acknowledgement. I have read and will comply with the above requirements regarding use of the Government issued cellular and satellite telephone devices. I understand my responsibilities regarding these devices and the information contained in them. I also understand and acknowledge what constitutes improper use and that I am subject to possible disciplinary action or financial obligation if I violate those guidelines and/or policies.

Date:

Employee Signature:

Acceptable Use Policy (AUP): Wireless Devices

11. I was issued the following wireless device(s):

Device Type: Smart Phone

IMEI:

Make/Model: Apple iPhone XR

ICCID #:

Serial #:

Phone #:

Rank/Grade

Signature

Date

=====

To Return the Device, please complete the fields below

Signature for Turn-In of Device

Date

DOD MOBILITY UNCLASSIFIED CAPABILITY (DMUC)

DMUC End User License Agreement

Last Name:

First Name:

Organization:

**Commercial /
DSN Phone Number:**

**NIPR Email
Address:**

Device:

IMEI:

DEVICE AND NETWORK SECURITY

- You are NOT authorized to connect a DMUC mobile device to any government or personal computer or laptop.
- Unapproved connections of the device will result in non-compliance and quarantine.
- Your device will be quarantined if you make any changes to it that would prohibit device management by DMUC.
- Devices MUST be used and managed in accordance with DoD/local security and wireless policies and mandated device settings (e.g., device supervision).
- You MUST not engage in any activity that interferes with the DoD network or any services available on the DoD network.
- Removable media (e.g., SD card, micro-SD card) are not authorized for use with your DMUC device.
- Personally Identifiable Information (PII), Protected Health Information (PHI), Controlled Unclassified Information (CUI), or any For-Official-Use-Only (FOUO) documents MUST not be transmitted to a non-Government controlled entity.
- Only update your mobile device operating system (i.e., iOS, Android) when notified by DISA.
- Devices report to the MDM every four hours (when powered on and connected to Wi-Fi or cellular data). Devices that have not 'checked in' to the MDM in over 30 days will be quarantined.
- Classified material is NOT authorized on the device. Contact your security manager for all security violations.
- Device MUST be turned off during any classified discussions.
- Device MUST NOT be used within three meters (nine feet) of a Secret Internet Protocol Router Network workstation.
- If you suspect your device has been compromised, immediately turn off the device and open a trouble ticket with the help desk at your local command and contact your security manager. A compromising event may include but it not be limited to: unauthorized password change, function or feature change, mobile applications (apps) unexpectedly appearing on the device, etc. If it is determined that the device has been compromised it will be wiped of its data, apps, and the service suspended.
- Commercial Wi-Fi networking is allowed only on trusted Wi-Fi networks with WPA2-Personal security. A trusted commercial Wi-Fi network, in accordance with Command Policy V2R3 STIG WIR-SPP-010, is defined as a site-managed Wi-Fi access point connected to the internet only (Internet Gateway Only Connection) or a home Wi-Fi network (user managed). Public or hotel hotspots are NOT allowed.
- When using a DMUC mobile device's hotspot, WPA2 encryption must be enabled and you must change the device name to something that is not meaningful (e.g., site name, product name, room number, end user's name) and change the manufacturer's default hotspot password before use. The hotspot must be turned off when not in use.
- You must adhere to the password complexity policy when you provision the device and this feature must remain enabled. All Apple iOS passcodes and Samsung device passwords must have a minimum of six (6) non-sequential characters. Samsung Galaxy Knox passwords must have a minimum of six (6) characters, which is the minimum allowed by MobileIron. Disabling or not enabling this feature during the provisioning process will flag your device as non-compliant and your device will be wiped.



DOD MOBILITY UNCLASSIFIED CAPABILITY (DMUC)

DMUC End User License Agreement

DEVICE FUNCTIONALITIES / CAPABILITIES

- Global Positioning System (GPS) is available for use on your device and can ONLY be used with approved apps and must be turned off when not in use. NOTE - GPS is a tracking device while it is active; therefore, you must check with your OPSEC office for guidance on using this feature, prior to travelling outside the United States.
- You are not authorized to add 3rd party email accounts nor sync contacts or calendar events between public apps to the device (e.g., Google Gmail, Microsoft Hotmail, Yahoo! mail).
- You are not authorized to enter developer mode or to print from your device.
- Screenshots are enabled on DMUC iOS devices. Use caution and discretion when using this function within both managed and unmanaged apps. Controlled Unclassified Information (CUI) can inadvertently be shared with unknown recipients.
- DISA maintains a list of authorized apps in the Mobile Application Store (MAS):
 - Managed apps (can process CUI): DoD Apps for iOS devices and Samsung Knox Workspace for Android devices
 - Unmanaged apps (MUST NOT process CUI): Personal Use Mobile Apps (P.U.M.A.) for iOS devices and MobileIron Apps@Work for Android devices
- Downloading unapproved or third-party apps may result in your device being flagged for non-compliance, quarantined, and potentially removed from the DMUC MDM.
- The iOS 13 STIG requires that all iOS and iPadOS devices be 'supervised.' Supervision provides a higher level of device management for organization-owned iOS and iPadOS devices. Tier I administrators can 'supervise' devices using Apple Business Manager (ABM).

The following features on Apple devices are NOT approved for use and MUST NOT be enabled:

Apple Devices:

- Sharing location data via iCloud
- iCloud backups
- Find My Friends and Find My iPhone in the Find My app*
- Storing PII in the Health App
- Apple Pay
- Sending Diagnostic data
- Associating payment information with Apple ID

The following features on Samsung devices are NOT approved for use and MUST NOT be enabled:

Samsung Devices:

- S Voice Mobile Assistant
- USB Storage
- Export Knox Calendar/Contacts to Personal mode
- Nearby devices
- Screen mirroring
- Manual date/time change
- Wi-Fi direct
- Physical/USB Wi-Fi Tethering
- Bluetooth File Transfer
- Message Preview on lock screen
- Multi-user mode (tablets only)
- Smart Lock
- Android Device Manager
- Development Mode
- Set up/enabling a Google account*
- Set up/enabling a Samsung account*
- Find my Mobile*
- Sending Google Crash Reports*
- Sending Diagnostic or Usage Data*
- Carrier backups or cloud-based capabilities
- Fingerprint authentication is authorized for Knox Workspace, but NOT for accessing the Samsung Android device
- Moving DoD Enterprise Email (DEE) calendar information outside of the Knox Workspace

*User Setup Guide is located on the Mobility Service Portal with instructions on skipping these steps to ensure they are not created

ACCOUNTABILITY OF GOVERNMENT MOBILE DEVICES:

- Users are responsible for the safekeeping and accountability of their device. Failure to do so may result in action taken by your organization's policy.
- You will not use the device in any manner that would constitute a criminal offense or give rise to civil liabilities.
- You are required to factory reset your device before turning in. For Android devices, make sure the Google account is removed from the device. If the existing Google account is not removed, new users will not be able to set up their new device and the Android device will be bricked due to the Samsung Factory Reset Protection (FRP).
- DoD Directive 5500.07 Standards of Conduct are applicable to mobile device use.

By signing my name below, I affirm that I have read, understand, and agree to comply with the restrictions and requirements set forth in this agreement and understand the DoD-funded mobile device services are For Official Use Only. I will abide by the rules governing proper use and security of the government mobile device assigned to me.

Signature:

Date:



Last Updated on 4 Feb 2020

DOD MOBILITY UNCLASSIFIED CAPABILITY (DMUC)

DMUC End User License Agreement

ANNEX

U.S. GOVERNMENT INFORMATION SYSTEMS

DoD CIO Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," May 9, 2008 Requirements Incorporating Change 5, September 25, 2013:

By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems.

You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government-authorized use only.

You consent to the following conditions:

- The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the U.S. Government may inspect and seize data stored on this information system.
- Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose.
- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests—not for your personal benefit or privacy.
- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
- Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
- The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
- Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
- Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
- A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
- These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (i.e., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.
- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provides a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

