DOD MOBILITY CLASSIFIED CAPABILITY – SECRET (DMCC-S) ANDROID DEVICE AND WINDOWS DATA-AT-REST – SECRET (WINDAR-S) USER AGREEMENT (UA) (Version 4.5)

Note: This information may be used to contact a DMCC-S device user in the event of a security incident or an emergency.

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. 301; 10 U.S.C. 131. PRINCIPAL PURPOSE(S): Gives the user of the DMCC-S Android and WINDAR-S device usage and security awareness training about the device. Shows user's agreement to use the device in accordance with security and wireless policies. Information provided by the user is needed for inventory control of the device, to verify compliance with DoD requirements for accountability of classified information and COMSEC material, and provides user emergency contact information if the device is lost, stolen, otherwise compromised, or requires reconfiguration due to security policy changes. ROUTINE USE(S): As stated in in this section. DISCLOSURE: Voluntary; however, failure to provide the requested information will result in denial of issuance of a DMCC-S Android and WINDAR-S device.

PART I - USER AND AUTHORIZED INDIVIDUAL (AI) INFORMATION

NOTE: Enter the user's information in **Blocks 1-10**. **Blocks 5-6** will serve as the mailing address for the device. A justification statement must be included in **Block 11**. The user's Organization POC or Supervisor must indicate their concurrence with the contents of this UA by completing **Blocks 24-27**. The user's security manager must validate the clearances of the user and AIs by completing **Blocks 28-31**. The user named below can be current government civilian, military personnel, or contractor. **Contractors** listed as a user or an AI are responsible for ensuring their issuing agency completed the mandatory Risk Acceptance Letter (RAL) from the Defense Counterintelligence and Security Agency (DCSA) which authorizes the identified personnel to possess and operate a classified device. Refer to DCSA's Assessment and Authorization Process Manual version 2.1 (or current version) for additional information and templates for agencies to use as guides (and tailor, as applicable).

1. Last Name	**2. First Name**	**3. Rank/Grade**
4. Organization/Agency	**5. Mailing Address**	**6. City, State, Zip Code**
7. Commercial Telephone Number	**8. Alternate Telephone Number**	**9. Classified Telephone Number (Specify classification)**

10. Enter the user's official email addresses below:

a. NIPRNet Email:

b. SIPRNet Email:

11. Mission Need/Justification Statement (Unclassified):

12. Authorized Individual(s) AIs (Required): The individual(s) named below can be current government civilian, military personnel, or contractor authorized to act on the user's behalf for the DMCC-S service. A user can identify and name up to **three (3)** AIs (this is not a requirement). **All** AIs named below **must sign in Part III of this UA** to acknowledge they read, understand the restrictions and requirements set forth in this UA, by the AI's organization (to include participation in organizational training), and ANNEX A, and that the AI agrees to comply with the same. The AIs may be members of a user's Communications Team or Tier I Service Desk (that meet the minimum requirements). As noted above, contractors listed as AIs are responsible for ensuring their issuing agency completes the mandatory RAL.

- A user's Primary AI (identified in **Blocks 12 a-h**) will be the individual responsible for the device after the user, may be in possession, and can operate the device to support the user (e.g., performs a test call to verify the device is operational).
- ALL provisions and requirements in the UA apply to the AIs. The user **MUST notify and submit a NEW**, signed UA to their organization's designated POCs and the Provisioning Team if **ANY** of the AIs change. (Devices must be returned for reprovisioning due to security requirements if the user or any of the AIs change.)
- By identifying AIs, the user concurs with the statement: I understand AIs are responsible for receiving and managing my device, hotspot, authentication password(s), communication related to troubleshooting and potential incidents, and information resulting from such access.

Check if NO AIs (do NOT complete 12 a-x): □ **User must initial here to indicate no AI:**

AI #1 (Primary): Enter the name and contact information for the first (primary) AI in **Blocks 12 a-h** below:

a. Last Name: **b. First Name:** **c. Rank/Grade:**

d. Organization/Agency: **e. Commercial Telephone Number:** **f. Classified Telephone Number:**

g. NIPRNet Email:

h. SIPRNet Email:

AI #2: Enter the name and contact information for the second AI in **Blocks 12 i-p** below:

i. Last Name: **j. First Name:** **k. Rank/Grade:**

l. Organization/Agency: **m. Commercial Telephone Number:** **n. Classified Telephone Number:**

o. NIPRNet Email:

p. SIPRNet Email:

AI #3: Enter the name and contact information for the third AI in **Blocks 12 q-x** below:

q. Last Name: **r. F irst Name:** **s. Rank/Grade:**

t. Organization/Agency: **u. Commercial Telephone Number:** **v. Classified Telephone Number:**

w. NIPRNet Email:

x. **SIPRNet Email:**

3. Authorized Service Interruption (ASI) POC (Required): The group mailbox (recommended) or individual identified below must be a current U.S. government civilian or member of U.S. military. The information and email addresses listed below must be current and authorized to send and receive communication and notifications related to DMCC-S ASIs for the individual named in Part I of this UA. Full name required if POC is an individual.

a. Group Mailbox/Full Name:

b. NIPRNet Email:

c. SIPRNet Email:

14. Communications Spot (COMSPOT) POC (Required): The group mailbox (recommended) or individual identified below must be a current U.S. government civilian or member of the U.S. military. The information and email addresses listed below must be current and authorized to send and receive communication and notifications related to DMCC-S COMSPOTs for the individual named in Part I of this UA. Full name required if POC is an individual.

a. Group Mailbox/Full Name:

b. NIPRNet Email:

c. SIPRNet Email:

PART II – DMCC-S INFORMATION

15. The following preventive measures are requirements to ensure that use of a DMCC-S device (includes Android and WINDAR-S) and referred to as an End User Device (EUD) or device, does not result in the release of classified DoD information to unauthorized persons. Unless explicitly stated otherwise, requirements in this UA apply to both DMCC-S Android and WINDAR-S users. Please refer to Section aa for DMCC-S Android device specific requirements and Section bb for WINDAR-S device specific requirements. Any questions should be directed to the user's authorized security official or Tier I.

I have been issued a DMCC-S Android or WINDAR-S device. I agree to abide by the United States Government rules and regulations in the Joint Ethics Regulation, DOD 5500.7-R as they apply to my use of this Government device. In addition, I acknowledge and consent to the terms carried in the "DoD Notice and Consent Provision" (found in the **ANNEX** portion of this

UA). I acknowledge and accept that modifications and enhancements to the DMCC-S environment may occur without prior notice.

I acknowledge that I have read, understand the restrictions and requirements set forth in this UA, by my organization to include my annual cybersecurity training and any additional cybersecurity training required by my organization and **ANNEX A**, and that I agree to comply with the same. I acknowledge that intentional violation of these terms may result in seizure of my DMCC-S device, and/or adverse administrative action, which can include criminal law enforcement action under some circumstances depending on the activity, for instance a military member for dereliction of duty. I understand that I must complete and return this signed UA prior to using the device and hotspot.

I understand and agree to the following:

a. Only authorized and appropriately cleared users, administrators, and security personnel can have physical access to an EUD and hotspot; this applies when in and not in a classified state. I have a valid justification for use of the DMCC-S service and am responsible for obtaining my organization's approval prior to requesting DMCC-S service. I understand DISA may contact me or my organization to validate my organization's approval at any time and I am responsible for providing this information immediately upon request.

b. I have an active security clearance at the Secret level or higher and must maintain this clearance as long as this device is assigned to me. If my clearance is revoked or suspended after I have been issued this device, I will contact my organization's authorized security representative for additional guidance and notify my organization's authorized Points of Contact (POCs) (which may include the Security Manager, Tier I Service Desk, or Communications Team).

c. Should my job duties no longer require use of the device or if I wish to permanently relinquish the device, I will notify DISA DoD Enterprise Mobility Team and the Provisioning Team to ensure my device is removed from the network. I will coordinate the return of my device, hotspot, and peripherals with my organization's authorized POCs (which may include the Security Manager, Tier I Service Desk, or Communications Team) in accordance with (IAW) my organization's turn-in requirements for classified devices. Refer to the DoD Mobility Commercial Device Disposal Plan for turn-in instructions located on the DoD Mobility Service Portal (MSP) for more information (Common Access Card (CAC) authentication required). If you are unable to use a CAC for access, please see the following link to the Contact us on DISA.mil: https://disa.mil/About/Contact.

d. The device and hotspot must be returned to the Provisioning Team for reassignment to a new user or if any AIs change. (Returns must be made IAW the Device Return Procedures. Refer to the DMCC User Guides on the MSP for more information (CAC authentication required). If you are unable to use a CAC for access, please see the following link to the Contact us on DISA.mil: https://disa.mil/About/Contact. I am not authorized to reassign or transfer responsibility for the device, hotspot, or peripherals. I must notify the Provisioning Team and submit a new, signed UA to the Provisioning Team if any individual identified as my AI in **Block 12** of this UA changes.

e. The device is only approved for use up to Secret voice and data, and at no time may it be used for processing information at a higher classification level than Secret. Such processing is prohibited, constitutes a security violation, and could lead to administrative action, seizure of the device, and/or referral to the appropriate criminal law enforcement authorities.

f. When a user receives approval to connect more than one device to a single hotspot, all devices paired to the hotspot must be approved to operate at the same classification level (no devices operating at different classification levels or multi-classification level devices).

g. The user must ensure that no classified data shall be put into the file's metadata (to include the filename).

h. I will not draw attention to the classification level of the device and hotspot. I will not mark the device and hotspot with an external, visible classification marking. I will only personalize the device and hotspot using an approved method for customization (this may include stickers that do not indicate classification, discreet markings, wallpaper (if permissible), or other visible means of personalization). I understand that I am not required to carry a courier card with the device and hotspot.

i. I will not use the device when I have access to a secure landline or a SIPRNet terminal. I shall turn off the device when not actively utilized (to include placing calls, sending instant messages, using the internet browser). I will not connect the device, hotspot, or peripherals to any computer, laptop, printer, device, or other external connection unless explicitly approved by the Authorizing Official (AO) for use with the device. This requirement applies to government, contractor, personal, and all equipment types (to include unclassified and all classification levels).

j. I understand it is my responsibility to apply operations security (OPSEC) countermeasures and assess risk, in order to avoid vulnerabilities from being exploited by an adversary. I will ensure sufficient privacy and isolation from others prior to using the device in classified mode and maintain awareness of my surroundings and proximity to uncleared individuals to minimize compromise of classified information. I will ensure the device and hotspot are concealed, especially when not in a secure location.

k. I understand that use of the device outside of a secure classified area should be restricted, unless I have determined it is critical to the mission and all other alternatives have been considered. I shall seclude myself from the general population when operating the device. I will not use the device in a residence or hotel (inside or outside of the United States) that may be insecure. I will exercise diligence when traveling in foreign countries with respect to criminals and local intelligence efforts to target the device for the information it contains. (Reference: DoD CIO Memorandum (Memo.) for Security and Operational

Guidance for Classified Portable Electronic Devices (PEDs), dated 25 Sep 2015).

l. I will ensure individuals without a need to know (NTK), and all unauthorized individuals are unable to hear or view any information on the device and hotspot, especially after the device has been authenticated. I will remain aware of potential threats and security vulnerabilities.

m. I will avoid using the device and hotspot while taking public transport and will check surroundings for video monitoring and recording devices. (Reference, DoD CIO Memo. for Security and Operational Guidance for Classified PEDs, dated 25 Sept 2015).

n. I will adhere to the device control measures to include those outlined below:

- I must maintain continuous physical control of the device and hotspot or store in a locked container, following the requirements and specifications established by the AO, to minimize the possibility of loss, theft, unauthorized use, and tampering. Minimum standards for storing the device and hotspot when not in the user's direct physical control are in a locked container, only accessible to the user (e.g., a desk drawer, cabinet, or the user's locked residence) or individual specifically authorized in this UA.
- I will maintain positive physical control over the device(s) and hotspot(s) assigned to me. I will remain aware of my surroundings and ensure an adequate physical standoff distance to mitigate threats associated with physical proximity. Proximity-related threats may include (but not limited to): "smart home" (such as Alexa-like devices), Internet-of-Things (IoT), wearable fitness trackers, and devices with active Near Field Communication (NFC).
- The physical standoff distance for the device and/or hotspot is at least 15 feet. Users are responsible for ensuring that all proximity-related threats are maintained at a distance of at least 15 feet and, to mitigate interaction with the device and hotspot, remain in a separate room throughout the duration of classified device uses. Users may use their DMCC-S or WINDAR-S device and/or hotspot three feet or more from an authorized, government issued Non-classified Internet Protocol Router Network (NIPRNet) or DoD Mobility Unclassified Capability (DMUC) device. Users must ensure that all devices with unverified distances for recording and listening capabilities remain powered down, power sources removed and recording and listening capabilities disabled throughout the entire duration of classified device use. If an unauthorized party takes possession of the device and hotspot (or the device and hotspot are out of my direct line of sight) and is suspected of performing activities with the device and hotspot without my knowledge, the device and hotspot are considered compromised.
- The device and hotspot must remain with the user during commercial travel. The device and hotspot must be powered down before they are handled by an unauthorized individual (e.g., customs). If an unauthorized individual requires that the device is powered on for inspection, the device must be re-booted before use. The user must inspect the device and hotspot before use if they are handled by an unauthorized individual.
- The following locations are not approved for storing the device and hotspot: leaving unattended or locked in an airport (to include checked luggage), train station, bus station, public locker, or unoccupied vehicle (even in a locked compartment).
- I understand the device and hotspot are considered lost as established by the AO when outside of my continuous physical control. (Users must follow their organization and AO's guidance for maintaining continuous physical control of their device and hotspot.)
- I shall inspect the device and hotspot for signs of tampering: routinely and immediately after I regain possession if the device and hotspot are out of my line of sight or there is an interruption in continuous physical control. Potential signs of tampering include pry marks, unexplained behavior, discoloration, changes to the device and hotspot appearance, and other examples defined by my organization and AO.
- I will report the absence of expected notification prompts immediately. Examples of prompts expected (and reportable if missing on the device) include: the DoD Standard Mandatory Notice and Consent Banner and prompt for authentication password.
- I will ensure the device and hotspot go through inspection for tampering if lost and recovered. I must receive approval prior to reuse of the device. I must follow the procedures outlined by the AO to determine if the device has been tampered with or substituted (in order to mitigate the risks associated with reuse after being out of my control) and if compromised, the device and hotspot may be destroyed.
- I understand that although the data at rest (DAR) solution can protect the confidentiality of data and render the device unclassified, it does not protect the integrity of the device outside of the control of approved users.

o. I will immediately report any signs of suspected or known unauthorized use or tampering IAW with my organization's policy, the AO, and described within this UA. I understand that this may result in the device being disabled, immediately removed from the network, and sent for forensic analysis, and tamper detection. Compromised devices and hotspots will be destroyed IAW the requirements set forth by my organization, AO, and the UA.

p. Suspected or actual incidents of tampering must be reported IAW the organization's AO, Level 1 Service Desk, and guidance required by this UA to report the incident to DISA to have the device removed from the network. Mission Partner (MP) Service Desks and DISA users call DISA's Global Service Desk (GSD) (24x7): 1-844-DISA-HLP (1-844-347-2457) (option 4). I understand that incident and problem resolution may require the device be sent back for reprovisioning. Devices that require reprovisioning will be factory reset and/or cryptographically erased and as a result, reprovisioned devices will not retain user data.

q. I will perform the following to maintain the device and hotspot:

- For devices and retransmission devices that remain on and in a sustained authenticated state (defined as **8** or more hours within a **24**-hour period), I will restart the device and hotspot at least once a day.
- Users are reminded that if they do not login or update their device regularly, their device may have issues when they first login after an extended period.
- I understand if the device and user do not connect to the network in **45** calendar days, the device's network and user's account access may be impacted to include conditional access or **temporarily disabled**, and the impacted user will be required to contact Tier I or individual authorized by my organization to have it reenabled.
- I understand if the device and user do not connect to the network in **60** calendar days, the device's network and user's account access may be **permanently disabled**, and the impacted user will be required to contact Tier I to coordinate the delivery of the device back to a provisioning center for reactivation.
- Users must not allow the device's battery to fully deplete. If the device's battery is in a fully depleted state for more than **24** hours the device may become inoperable. DISA DoD Enterprise Mobility Team suggests turning off the device during periods of non-use (less than **10** calendar days) with a charge state of at least 75%.
- The Android device must be used for a call (or test call) at least once every **10** calendar days to establish a date-time sync with the gateway, failure to conduct this may cause the device to lose sync with the gateway and require reprovisioning.
- I understand that disablement or deactivation of the device and hotspot will not necessarily stop billing services in DSF. Refer to DISA Storefront's (DSF) Reference Materials for more information.) for more information.

r. **Device Certificate Expiration Period**: Effective 28 January 2022, the device certificate expiration returned to 36 months from the date the certificate is generated during the provisioning process. I am prohibited from using a device and hotspot with an expired certificate until the device and hotspot have been returned and reprovisioned by the Provisioning Team.

s. I affirm my completion of all required user training, including instruction on proper use, protection of the device, retransmission device, and their security features prior to using the device and hotspot. Required training includes DoD and Agency requirements. Refer to Section cc for sources of authoritative guidance.

t. I will use the charging cables provided to charge the device and hotspot. A computing device, such as a laptop, is NOT an authorized power source and is strictly prohibited.

u. I will only use the peripherals approved for use with my device and hotspot. I will contact my Authorizing Official (AO) or their designated representative with questions about peripherals if the peripheral is not authorized for use with a classified device. Attempts to use or connect the device and/or hotspot (including the AT&T Nighthawk hotspot) to all forms of external media (to include MicroSD cards and USB drives) are explicitly prohibited. A user is prohibited from using peripherals that use wireless or data transfer functions, to include any Subscriber Identity Module (SIM) card, other than those provided or authorized for use with the device and hotspot. Effective 1 June 2022, use of the Samsung Multi-Port adapter may be used to increase the number of available ports on the WINDAR-S or DMCC-S Android devices. Personnel are prohibited from installing any external drivers and must submit a request to unblock ports if the ports are blocked by default. All peripherals must be plug-n-play and cannot function as "smart" devices or connect to the Internet of Things (IoT).

v. Only US-based, government-procured SIM cards provided are intended for use with the retransmission device. Any attempts to use a foreign SIM card will be viewed as a security violation which may result in adverse actions to include termination. Please refer to your organization's policy for replacement peripherals and contact your authorized security representative with any questions.

w. The devices and hotspots are government property and considered accountable. I will report lost, damaged, improperly destroyed, or potentially compromised devices to my security official and to the GSD (DSN 312-850-0032 or Commercial 1-844-347-2457) for investigation, evaluation, and reporting. This includes attempting to open any part of the device or hotspot that is not expressly authorized. In the event of damage (other than reasonable wear and tear), negligence or abuse, a DD Form 200 (Financial Liability Investigation of Property Loss) shall be prepared and processed. The incident shall be investigated immediately IAW local organizational accountability procedures.

x. I understand that I am prohibited from accessing and attempting to change the settings or configurations of my device, hotspot, or peripherals (if applicable). I am prohibited from attempting to unlock or change (to include altering, removing, and adding) the device and hotspot's settings or configurations unless expressly approved by an authorized government official (such as the AO) in writing. Prohibited setting and configuration changes include applications and software on the device or hotspot. Only authorized individuals, such as DISA support teams (to include members of the Provisioning Team and applicable service desk) can configure these settings.

y. I understand that due to the requirements necessary to protect classified data, warranty repair services from device manufacturer or third parties may not be used. I understand if service cannot be restored to an inoperable DMCC-S device, it will need to be disposed of IAW with the DoD Mobility Commercial Device Disposal Plan (CAC-enabled) and DoD regulatory guidelines. I understand that the replacement DMCC-S device costs are my responsibility regardless of length of service or circumstance.

z. I understand that DMCC-S service is highly dependent on non-assured public cellular services; environmental factors such as signal strength and network technology impact service levels.

aa. **DMCC-S Android device** specific requirements found below:

- The device is unclassified and considered high value until it is provisioned (keyed) and the device authenticates (using the password provided upon receipt of the device). Upon authentication, the device is classified Secret and must be protected IAW the requirements for information classified Secret. The device must still be managed at the Secret classification level after authentication, but in a locked or logged off state.
- The device screen will lock after the user initiates or after **two minutes idle** and the **Knox Workspace** will lock after 30 minutes. Note: Users have **12 hours** starting when they last used an application in the Knox Workspace, in which they will be able to receive calls while the device is in a locked state. After the prescribed time period, whether in an active call or not, users **must** enter the device and container passwords to remain in an existing, place, or receive a new call.
- The device authentication PIN and DAR password (if issued with the device) are treated as **CUI** when written down separately and **NOT** associated with the device. The device authentication PIN and/or DAR password (if issued with the device) are classified **SECRET** when associated with the device (stored with, attached to, etc.). The device authentication PIN and DAR password are classified **SECRET** when together (stored with, attached to, etc.), even if not associated with the device.
- I am responsible for securing the PIN and password IAW the requirements identified above, to include up to the **SECRET** classification. I will store the PIN and passcode in a separate container from the device and I will never mail, store, transport, or attach the PIN, password, or authentication tokens to the device or hotspot.
- I understand that the device will factory reset after entering the device screen lock PIN **incorrectly** 10 consecutive times. If a device factory resets, the device and hotspot must be reprovisioned before they can be used for classified calls.
- Effective 16 April 2024, the following peripherals are approved for use with DMCC-S Android devices:
  - i. Plug-n-play USB-C AKG headphones
  - ii. The S-Pen is authorized for use with the tablets
  - iii. The book cover keyboard with POGO connection is authorized with the tablets
  - iv. RJ-45 (Ethernet) cable is authorized for use for hotspot Ethernet offloading
  - v. Samsung USB Multi-Port adapter
  - vi. Universal Serial Bus (USB) Power Bank or External Power Source
  - vii. Battery Sleeve
- I understand the peripherals can only be purchased from a General Services Administration (GSA)-approved vendor and can only be plug-n-play.
- I understand the use of speakerphone is prohibited with the tablet and must use authorized headphones when placing or receiving calls or any type of voice communication (i.e., conference calling, voice mail, etc.).

bb. **WINDAR-S device** specific requirements found below:

- The device is unclassified until it is provisioned (keyed), booted (powered on) and the device encryption (BitLocker) password is authenticated. Upon user password authentication, the device is classified and must be handled at the **SECRET** level until powered off.
- User storage of classified data on this device is permitted but must be encrypted with the provided file encryption software installed on the device (Dell Data Protection Encryption). I shall place the device in screen lock mode or power down the device to engage BitLocker when the device is not in active use.
- If the device and hotspot are powered on and connected to the VPN, after a period of 12 consecutive hours of inactivity, the device will automatically shutdown to comply with security requirements. A user's programs or files may be negatively impacted (such as file loss) during if open during the automatic shutdown.
- I understand that during Quality Control, a DMCC-S authorized provisioner will send a test email from my SIPR email account on the DMCC-S device to a DISA Mobility PMO SIPRNet Mailbox to confirm proper setup.
- I understand that DMCC-S devices are maintained via the Defense Property Accountability System (DPAS), a DoD property management system. I will maintain accountability of my device(s) via DPAS and update sub-hand receipt(s) as required. If my organization is not one of the 32 DoD Agencies and Military Services using DPAS, I will receive DPAS GFE via lateral transfer to my organization's Accountable Property System of Record (APSR) and maintain GFE IAW my organization's Accountable Property Officer.
- I will not tamper with the WINDAR-S or retransmission device in any way. Attempting to change the configurations, performing unauthorized factory resets, using outside of an explicitly approved methods (for example, attempting or using settings on the device or hotspot (such as buttons on the top of the Nighthawk hotspot) or connecting the hotspot to devices not approved for use are prohibited).
- Effective 16 April 2024, the following peripherals are approved for use with WINDAR-S:

i. Personally owned computer monitors to WINDAR-S devices via Video Graphics Array (VGA) and Digital Video Interface (DVI) connections, but not a USB connection
ii. HDMI or Display Port connections are authorized if VGA and DVI are unavailable
iii. Personally owned USB type-A wired keyboards and mice
iv. Plug-n-play AKG headset
v. RJ-45 (Ethernet) cable is authorized for use for hotspot Ethernet offloading
vi. Samsung USB Multi-Port adapter
vii. USB Power Bank or External Power Source
viii. Battery Sleeve

- I understand the peripherals can only be purchased from a GSA-approved vendor and can only be plug-n-play.
- I will contact my local Service Desk to obtain technical support for any device malfunction and my authorized security authority with any questions.

cc. Users must follow DoD and organizational policy for use of peripherals and obtain approval/exemption from the AO and security manager prior to introducing and using in a government-controlled facility and/or with their DMCC-S and/or WINDAR-S device (usage policies apply to peripherals that ship or accompany select models of DMCC-S and WINDAR-S devices). Approved peripherals include USB/USB-C (including adapter) connected headphones, keyboards, and styluses. Resources include: DoD Issuances: (whs.mil); Risk Management Framework Knowledge Service (https://rmfks.osd.mil/); DoD Cyber Exchange (Cyber.mil); NSA's Telework and Mobile Security Guidance (nsa.gov).

dd. I acknowledge that I am responsible for use of all approved peripherals with my device. I will only connect a peripheral if my local security manager has approved the specific make and model of the peripheral for use on a classified information system (an example of a peripheral is headphones). The peripheral must meet the requirements outlined in this UA, official DoD, and organizational policy.

ee. Use of Bluetooth and/or Bluetooth-enabled devices is prohibited and/or restricted by DoD and organizational policy. I acknowledge that DMCC-S Android and WINDAR-S devices have Bluetooth disabled and I am prohibited from attempting to change or circumvent these configurations on the devices.

ff. I will return the device if I no longer require it for my job duties or I wish to permanently relinquish it. I will return the device, hotspot, and all accompanying peripherals to my organization IAW the DoD Mobility Commercial Device Disposal Plan (CAC-enabled) and DoD regulatory guidelines for management of classified device. My agency will only return the device to DISA if my device must be reprovisioned. However, I understand that DISA may request that I return the device and/or hotspot at any time to comply with mission or security requirements. Prior to returning my device, I will coordinate the return with my agency's applicable POC for property accountability and return the device IAW the Device Return Procedures. Refer to the DMCC User Guides available on the DoD Mobility Service Portal (MSP) (CAC authentication required) for more information. If you are unable to use a CAC for access, please see the following link to the Contact us on DISA.mil: https://disa.mil/About/Contact.

gg. Users are authorized to fully destroy the device, hotspot, and peripherals when in a hostile environment and destruction of the device and hotspot is required to prevent seizure by unauthorized individuals – destruction to prevent seizure must be reported immediately once in an appropriate location. The DoD Mobility Commercial Device Disposal Plan (CAC-enabled) provides guidance for disposal and recycling.

hh. User organizations are responsible for destroying a device, hotspot and peripherals that have been returned and is no longer in use as noted in item ff. The DoD Mobility Commercial Device Disposal Plan (CAC-enabled) provides guidance for disposal and recycling.

ii. Management of the records data on a user's device is the responsibility of the user and their organization and not the Mobility Program Office. It is the user's responsibility to follow the policy and guidance of their organization's records management requirement.

ANNEX A

STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS

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.

PART III – SIGNATURES

The user (the individual named in **Blocks 1-10**) must digitally sign in **Block 16** and date in **Block 17** below. The AI(s) must digitally sign and date in **Blocks 18-23** (as applicable). The user acknowledges the AIs signing below must be current government civilian, military personnel, or contractor and will be authorized to act on behalf of the user. The AI(s) are responsible for managing and receiving the user’s device, hotspot, authentication PIN, and communication related to troubleshooting and potential incidents.

16. Signature of User	**17. Date Signed (YYYYMMDD)**
18. Signature of AI #1 (Primary)	**19. Date Signed (YYYYMMDD)**
20. Signature of AI #2	**21. Date Signed (YYYYMMDD)**
22. Signature of AI #3	**23. Date Signed (YYYYMMDD)**

PART IV – ORGANIZATION POC OR SUPERVISOR APPROVAL

By signing below, I affirm that the user and AIs named in **Part I** of this UA meet the minimum requirements specified within this UA. Minimum requirements include required organizational-developed training on securing and operating the device and hotspot, guidance on tamper awareness and detection, and mandatory Information Assurance (IA) training required by the user's organization.

I understand that I am responsible for tracking the DMCC-S device users within my organization. I must notify my organization's designated POC and DISA (to include the Provisioning Team and DISA DoD Enterprise Mobility Team) when the user no longer requires access, and I am responsible for tracking and managing device returns IAW organizational guidance. I understand the DISA DoD Enterprise Mobility Team may request the user to relinquish their device and hotspot, without reason, at any time. Refer to the DMCC User Guides available on the MSP for contact and device return information (CAC authentication required). If you are unable to use a CAC for access, please see the following link to the Contact us on DISA.mil: https://disa.mil/About/Contact.

24. Org POC or Supervisor Last Name	**25. Org POC or Supervisor First Name**
26. Signature of Org POC or Supervisor	**27. Date Signed (YYYYMMDD)**

PART V – SECURITY MANAGER APPROVAL

By signing below, I affirm that the user and AIs named in Part I of this UA hold an active security clearance (**Secret** or higher).

28. Security Manager Last Name	**29. Security Manager First Name**
30. Signature of Security Manager	**31. Date Signed (YYYYMMDD)**