DOD MOBILITY CLASSIFIED CAPABILITY-TOP SECRET (DMCC-TS) USER AGREEMENT (UA) – Version 7.0

NOTE: This information may be used to contact a DMCC-TS 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): Identifies the user of the DoD Mobility Classified Capability-Top Secret (DMCC-TS) device as receiving usage and security awareness training governing use of the device and agreeing to use the device in accordance with security and wireless policies. This information is used for inventory control of the device, to verify compliance with DoD requirements regarding accountability of classified information and COMSEC material and provides user emergency contact information in the event that the device is lost, stolen, otherwise compromised, or requires a reconfiguration due to security policy changes. ROUTINE USE(S): None. DISCLOSURE: Voluntary; however, failure to provide the requested information will result in denial of issuance of a DMCC-TS device.

PART I - USER AND AUTHORIZED INDIVIDUAL INFORMATION

NOTE: Enter the user's information in **Blocks 1-12. Blocks 5-6** will serve as the mailing address for the device. If the user must remain anonymous due to mission need or security requirements, **you MUST** enter the name and contact information for the **PrimaryAuthorized Individual (AI)** acting on behalf of the user in **Blocks 1-10 AND** enter the **Primary AI's** contact information in **Block 13 a-h**. A justification statement must be included in **Block 11**. The security manager will indicate their concurrence with the contents of the User Agreement by completing **Blocks 24 to 27**. **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(Please specify classification)**

10. Enter the user's official e-mail addresses below:

a. NIPRNet E-mail:

b. SIPRNet E-mail:

c. JWICS E-Mail (if applicable):

11. Mission Need (Unclassified):

12. Number of Devices Requested for User:

13. Authorized Individual(s) (AIs): 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-TS 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 13 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 (ex. performs a test call to verify the device is operational). ALLprovisions and requirements in the UA apply to the AI(s). The user **MUST notify AND submit a NEW**, signed UA to the DoD Enterprise Mobility if **ANY** of the AIs change. (Devices must be returned for re-provisioning due to security requirements if the user or any of the AI change.)
- By identifying AIs, the user concurs with the statement: I understand the AI(s) are responsible for managing and receiving my device, hotspot, authentication PIN, and communication related to troubleshooting and potential incidents.

Check if NO Authorized Individuals (do NOT complete 13 a-x): ☐ **User must sign or initial here to indicate No AI:**

Authorized Individual #1 (Primary): Enter the name and contact information for the first (primary) AI in **Blocks 13a-h** below.

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

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

g. NIPRNet Email:

h. SIPRNet Email:

Authorized Individual #2: Enter the name and contact information for the second AI in **Blocks 13i-p** below.

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

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

o. NIPRNet Email:

p. SIPRNet Email:

Authorized Individual #3: Enter the name and contact information for the third AI in **Blocks 13 q-x** below.

q. Last Name: **r. First Name:** **s. Rank/Grade:**

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

w. NIPRNet Email:

x. SIPRNet Email:

14. Authorized Schedule Interruption (ASI) POC (Required): The group mailbox identified below is an official US government mailbox authorized to send and receive communication and notifications related to DMCC-TS ASIs for the individual named in **PartI** of this UA. (Name required if POC is an individual.)

a. Group Mailbox/Name:

b. NIPRNet Email:

c. SIPRNet Email:

15. COMSPOT POC (Required): The group mailbox identified below is an official US government mailbox authorized to send and receive COMSPOT communication related to DMCC-TS for the individual named in **Part I** of this UA. (Name required if POC is an individual.)

a. Group Mailbox/Name:

b. NIPRNet Email:

c. SIPRNet Email:

PART II – DMCC-TS INFORMATION

The following preventive measures are requirements to ensure that use of the DMCC-TS device – also referred to throughout as "device" – does not result in the release of classified DoD information to unauthorized persons.

By signing this agreement, I agree to abide by the United States Government rules and regulations carried in DoD 5500.7-R, "Joint Ethics Regulation" as they apply to my use of this Government device and I consent to the restrictions and requirements set forth in this Agreement and **Annex A**. I acknowledge that intentional violation of these terms may result in seizure of my DMCC-TS 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. I have an active **TOP SECRET (TS)** collateral clearance or higher and must maintain this clearance as long as I am assigned the device and hotspot. If my TS collateral clearance is revoked or suspended after I am issued the device, I will immediately contact my organization's authorized security authority, return the device in accordance with my organization'sestablished security procedures, and notify the DoD Enterprise Mobility.

b. I am responsible for obtaining my organization's approval prior to requesting, taking possession, and using the device and hotspot in any way. I am responsible for providing DoD Enterprise Mobility with my organization's justification immediately upon request. I understand DoD Enterprise Mobility may contact me or my organization to validate my

organization's approval at any time.

c. The device is Unclassified and considered high value until it is booted (powered on) and PIN authenticated. Upon user PIN authentication, the device is classified TS collateral and must be handled at the TS collateral classification level until powered off.

d. Only authorized and appropriately cleared users, administrators, and security personnel may have physical access to EUDswhen in a classified state.

e. The device is approved for up to TS collateral voice communication. Voice communication using the gateway/network maynever exceed the TS collateral level or be used for TS/Sensitive Compartmented Information (SCI) communication.

f. Discussing information at a classification level higher than TS collateral is prohibited and constitutes a security violation thatcan lead to administrative action, seizure of the device, and/or referral to the appropriate criminal law enforcement authorities.

g. The DMCC-TS service is voice only and improper device use protocols apply to use of the mobile hotspot provided with the device. User storage of classified data on the device is strictly prohibited and shall be considered spillage. Installation of applications or modification of the device is prohibited without the approval of the Authorizing Official (AO).

h. Users are **PROHIBITED** from connecting the device or hotspot to any Unclassified or Classified information system. Users must **never** connect unauthorized accessories/peripherals to the device or hotspot. (Unauthorized accessories notapproved for use include headphones with microphones.)

i. 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.)

j. The device does **NOT** permit emergency calls to 911.

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

l. Introducing the device into a secure facility shall be subject to the controls established by the presiding security authority. I am responsible for awareness and compliance with the local facility's security controls and procedures, and I will consult with the local security authority prior to bringing the device into a US government or other secured facility.

m. Use of the device and hotspot overseas should occur in a location or facility governed by the US whenever possible.

n. I will not use the device unless required by mission and when I have no alternative method to communicate classified information securely. I will seek an isolated location prior to authenticating to the device and placing or receiving a call.

o. I will not use the device when I have access to a landline or other method authorized for secure communication at the required classification level. I will only authenticate to the device when placing or expecting a secure voice call. I will place the device in screen lock mode when not in an active call and I will power down the device and hotspot when not expecting a call.

- Effective 1 Jun 2022, the device screen will lock upon initiation by the user or two (2) minutes idle. The Knox Workspace will lock after 30 minutes. After the device screen locks, users will have 12 hours 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 place or receive a new call.

p. I will remain aware of potential threats, security vulnerabilities, and proximity to individuals that may overhear voice conversations, view the screen or other components of the device and hotspot while it is authenticated. (Avoid using thedevice and hotspot while taking public transport and check surroundings for video monitoring or recording devices.)

q. I will not draw attention to the classification level of the device and hotspot. I will not mark the device and hotspot with andexternal, visible classification marking. I understand that I am not required to carry a courier card with the device and hotspot.

r. The device authentication PIN and Knox container password are treated as **CONTROLLED UNCLASSIFIED INFORMATION (CUI)** when written down separately and NOT associated with the device. The device authentication PIN and/or Knox container password are classified **TOP SECRET** when associated with the device (stored with, attached to, etc.). The device authentication PIN and/or Knox container password are classified **TOP SECRET** when together (stored with, attached to, etc.), even if not associated with the device. I am responsible for securing the PIN IAW the requirements identified above, to include up to the **TOP 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.

s. 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 an AO-approved, 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).

t. The physical standoff distance between 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 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.

u. While in use, the device screen will lock after the user initiates or after two (

v. Devices may be examined during a routine inspection at an authorized inspection point. If the device is out of my physical possession for more than 20 minutes or inspected for a non-standard period of time, I am responsible for reporting this fact immediately to my organization’s authorized security authority, Level 1 (L1) Service Desk, and DoD Enterprise Mobility to have the device removed from the network. (MP Service Desks call Comm: 1-844-DISA-HLP (1-844-347-2457/DSN: 850-0032) (Opt 4); DISA Internal Users call Comm: 1-844-DISA-HLP (1-844-347-2457/DSN: 850-0032) (Opt 4).)

w. I shall inspect the device and hotspot regularly for signs of tampering and unauthorized changes. If the device or hotspot isout of my physical line of sight, I will inspect the device and hotspot for signs of tampering and unauthorized use immediately after I regain physical possession. I will contact my organization’s security authority, L1, and the DoD Enterprise Mobility if there is any suspicion of compromise. I understand that compromised or devices suspected of compromise will be removed from the network immediately and submitted for forensic analysis.

x. I agree to comply with property accountability procedures found in DISA Instruction 270-165-08, DoD 5000.64 and periodic auditing deemed mandatory by DISA to verify continuing possession of DMCC-TS equipment. When a device is reported lost, damaged, or improperly destroyed, the incident will be reported to the organization's authorized security authority, L1,and DoD Enterprise Mobility and investigated immediately in accordance with local organizational accountability and incident reporting procedures.

y. Devices are government property and accountable devices. Attempting to open any part of the device is prohibited and shall be considered an incident that requires a full investigation. In the event of device or hotspot damage (other than fair wear and tear), negligence or abuse, a DD Form 200 (Financial Liability Investigation of Property Loss) shall be prepared and processed.

z. I understand that due to the processing of classified data, warranty repair services offered by the device manufacturer or third parties may not be used. I understand that if service desk troubleshooting and the DoD Enterprise Mobility (Tier III) cannot restore service to an inoperable DMCC-TS device, it will need to be disposed of in accordance with DPAS procedures and DoD regulatory guidelines. I understand that replacement costs are the responsibility of myself or my Authorized Individual(s), regardless of length of service or circumstance. For more information on proper disposal of a DMCC-TS device, please refer to DoD Enterprise Mobility guidance.

aa. I am not authorized to reassign or transfer responsibility for the device or hotspot. The device and hotspot must be returned to the DoD Enterprise Mobility for reassignment. DoD Enterprise Mobility may require the user to return the device for re- provisioning if the AI changes. I am responsible for notifying and submitting a new, signed UA to the DoD Mobility PMO if the individual(s) identified as my Authorized Individual(s) (AI) in **13** of this UA changes

bb. I understand the device certificates will expire **14 months** from the date of issuance. Once expired, the device must be returned to the DoD Enterprise Mobility for re-provisioning.

cc. Should I wish or need to permanently relinquish the device, I must return the device, hotspot, and peripherals to the DoD Enterprise Mobility. I will contact the DoD Enterprise Mobility to de-board prior to returning the device.

Users are authorized to perform a device wipe and then fully destroy the device and hotspot when in **a hostile environment** and destruction of the device and hotspot is required to **prevent** seizure by unauthorized individuals.

I understand that I must complete all required Information Assurance (IA) and user training (including instruction on proper use and protection of the device and its security features) prior to use. Refer to the DoD Mobility Service Portal (MSP) for more information (Common Access Card (CAC) authentication required).

Users should attempt to contact the presiding security authority before modifying or destroying the device or hotspot to the maximum extent possible. Users and the security authority are required to report any compromise, alteration, or destruction of the device or hotspot (once available/upon notification of the incident).

User 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. DoD Enterprise Mobility suggests turning off the DMCC-TS device during periods of non-use (less than 10 calendar days) with a charge state of at least 75%.

The device must be used for a call (or test call) at least once every **10** calendar days. If the device is not used for at least **1** call or test call within a period of **30** calendar days, its access to the network may be temporarily disabled and the user may be **removed** from the program. I understand that disablement or deactivation of the device and hotspot will not necessarily stop billing services in DISA Storefront (DSF). Refer to DSF's Reference Materials (Visual Walk Throughs) for more information.

I understand that if the DMCC-TS device does not connect to the network within **60** calendar days, its access to the network may be permanently disabled. (The device and hotspot should automatically connect to the network when turned on in accordance with standard operating procedures provided by the DoD Mobility PMO.) To re-activate the device, I am required to follow the appropriate escalation procedures to coordinate the delivery of the device back to a provisioning center. If applicable, disablement or deactivation of the device will not necessarily stop billing services.

DMCC-TS is a single threaded system with Level 2 support available **8x5 EST, Monday-Friday**. This device shouldNOT be **exclusively** used for any mission critical tasking due to lack of a COOP site and local fail over.

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.

o 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.

o 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 1-12**) must sign in **Block 16** and date **Block 17** below. The AI(s) must sign in **Blocks 18-23** (as applicable). The user acknowledges the individual(s) signing below must be current government civilian or military personnel and will be authorized to act on behalf of the user for the DMCC-TS service. 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 Authorized Individual #1 (Primary)	**19.** Date Signed (YYYYMMDD)
20. Signature of Authorized Individual #2	**21.** Date Signed (YYYYMMDD)
22. Signature of Authorized Individual #3	**23.** Date Signed (YYYYMMDD)

PART IV – SECURITY MANAGER APPROVAL

By signing below, I affirm that the individual(s) named and AI(s) identified in **Part I** of this Agreement meet the minimum requirements specified within this UA. Minimum requirements include security clearance (**TOP SECRET** collateral or higher), required training on securing and operating the device and hotspot, and mandatory training required by the user's organization.
I understand that I am responsible for tracking the DMCC-TS users within my organization and I must notify DoD Enterprise Mobility when the user no longer requires access. I understand that DoD Enterprise Mobility may request the user relinquish their device and hotspot, without reason, at any time.

24. Security Manager Last Name	**25.** Security Manager First Name
26. Signature of Security Manager	**27.** Date Signed (YYYYMMDD)