

26a. NAME (<i>Last, First, Middle Initial</i>)	26b. SOCIAL SECURITY NUMBER
--	-----------------------------

27. OPTIONAL INFORMATION (*Additional information*)

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION	28a. DATE OF INVESTIGATION (<i>YYYYMMDD</i>)		
28b. CLEARANCE LEVEL	28c. IT LEVEL DESIGNATION <input type="checkbox"/> LEVEL I <input type="checkbox"/> LEVEL II <input type="checkbox"/> LEVEL III		
29. VERIFIED BY (<i>Print name</i>)	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE (<i>YYYYMMDD</i>)

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED (<i>YYYYMMDD</i>)	PROCESSED BY (<i>Print name and sign</i>)	DATE (<i>YYYYMMDD</i>)
DATE REVALIDATED (<i>YYYYMMDD</i>)	REVALIDATED BY (<i>Print name and sign</i>)	DATE (<i>YYYYMMDD</i>)

DD Form 2875 Part II Continuation of Block 27 for CAMS-ME Use

PART II – Item 27 Optional Information (This item is intended to add additional information as required.)

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. **NOTE:** Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

27. ACCESS REQUESTED (Site specific system or application information)	
a. SYSTEM(S) CAMS – ME	b. DOMAIN(S) N/A for CAMS-ME
c. SERVER(S) N/A for CAMS-ME	
d. APPLICATION(S) OR MODULE(S) CAMS-ME Portal CAMS-ME GUI (CITRIX) CAMS-ME Project Team CAMS-ME Direct Database Access (Privileged)	h. COMPLETE FOR ALL ACCESS REQUESTS: User's Name: _____ User's SSN: _____ User's Org Code & Location: _____ User's Component Agency: Army [] Navy [] Air Force [] Other Defense Agency [] User's Birth month and day (MMDD): _____ User EDI Personal Identifier: _____ User has completed all required Military Equipment Valuation & CAMS-ME training prior to requesting access. ___ YES ___ NO User must complete and provide their signed acknowledgement that they have read and they understand all System Security Rules of Behavior for CAMS-ME. The signed acknowledgement must be attached to the submitted DD Form 2875.
e. DIRECTORIES N/A for CAMS-ME	
f. FILES (System to System) N/A for CAMS-ME	i. PRINTERS N/A for CAMS-ME:
g. DATASETS N/A for CAMS-ME	j. FOR MODIFIED PARTS II ONLY (COMPLETE ONLY FOR CHANGES): I certify that I have received Information Assurance Awareness training within the last year. User's Signature/Date: _____ I certify that I have read (or been briefed on) the system rules of behavior and the security and privacy notice and have completed and signed a user's security and privacy training statement. User's Signature/Date: _____ I certify that this user requires access as requested. Supervisor's Signature/Date: _____ Supervisor's Printed Name: _____ I certify that this user has a current DD Form 2875 on file. FIO's Signature/Date: _____ FIO's Printed Name: _____

DD Form 2875 Part II Continuation of Block 27 for CAMS-ME Use

PART II – Item 27 Optional Information (This item is intended to add additional information as required.)

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. **NOTE:** Records may be maintained in both electronic and/or paper form.
ROUTINE USES: None.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

CAMS-ME

<p>27k. OPTIONAL USE Continued. NOTE: Only one profile may be selected. Selected profile cannot conflict with user's Component Agency.</p> <p>CAMS-ME Portal Profiles</p> <p><u>ITEM MANAGER</u></p> <p>(2101) Army (1701) Navy (5701) Air Force (9701) Other Defense Agency</p> <p><u>PROPERTY MANAGEMENT ANALYST</u></p> <p>(2102) Army (1702) Navy (5702) Air Force (9702) Other Defense Agency</p> <p><u>PROPERTY MANAGER</u></p> <p>(2103) Army (1703) Navy (5703) Air Force (9703) Other Defense Agency</p> <p><u>PROPERTY MANAGEMENT SUPERVISOR</u></p> <p>(2104) Army (1704) Navy (5704) Air Force (9704) Other Defense Agency</p> <p>Note: For role descriptions see the CAMS-ME Portal User Profiles Web Page (click here).</p>	<p>CAMS-ME GUI Profiles</p> <p><i>(Note: Each user assigned to a CAMS-ME GUI profile will also be granted Portal access via profile (102) Valuation Resource)</i></p> <p><u>GUI FINANCIAL MANAGEMENT SUPERVISOR</u></p> <p>(2107) Army (1707) Navy (5707) Air Force (9707) Other Defense Agency</p> <p><u>ADMINISTRATORS</u></p> <p>(104) Valuation Administrator (OSD)</p> <p><u>GUI VALUATION ADMINISTRATOR</u></p> <p>(2106) Army (1706) Navy (5706) Air Force (9706) Other Defense Agency</p> <p>Note: For role descriptions see the CAMS-ME GUI User Profiles Web Page (click here).</p>	<p>CAMS-ME Project Team Profiles</p> <p><i>(Note: Each user assigned to a Project Team profile will also be granted Portal access via profile (102) Valuation Resource)</i></p> <p>(105) Central Administrator (107) Operations Property Manager (151) Help Desk (152) Security (154) Level 3 Display-only Profile (156) Security Auditor (161) Portal Object Manager Profile</p> <p>CAMS-ME Privileged Profiles (DBA/SA)</p> <p>(153) BASIS</p>
---	---	--

INSTRUCTIONS FOR THE PRE-POPULATED CAMS-ME PORTAL DD FORM 2875

The following instructions have been modified. The original standard instructions for filling out the DD 2875 are in non-bold type. All instructions specifically for CAMS-ME Portal Users are in bold. Each user will be required to complete a DD 2875, including a Part II supplement, along with the signature page, J-5, of the System Rules of Behavior attesting that the user has read and agrees to the Rules of Behavior.

IMPORTANT: Please note that when completing a DD Form 2875, nothing can be scratched out and there cannot be any markings that could be interpreted as an alteration of the form or its contents.

The following information must be provided by the user when establishing, modifying, or deactivating their CAMS-ME Portal User ID.

Type of Request: Select "Initial" for new access requests. Items 1-12 are all required items for new access requests. If request is to "Deactivate" a user account, provide the "User ID." Enter the "Date" of request. If the user is requesting a "Modification" of his assigned profile and has no other changes to his account information, only the Part II Supplement is required. Please submit the entire packet if there are other changes to the user account information.

System Name (Platform or Applications): Specify "MEV CAMS-ME Rel 1.1 Portal User."

Location: Specify "DISA Ogden, UT."

A. PART I: To be completed by User/Requestor

- (1) Name: Enter the last name, first name, and middle initial of the user.
(2) Social Security Number: Enter the social security number of user.
(3) Organization: Provide the user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).
(4) Office Symbol/Department: Provide the office symbol within the current organization (i.e. SDI). Enter your Government Office Symbol. Do not leave blank.
(5) Phone (DSN or Commercial): Provide the 7-digit Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate the 10-digit commercial number of the user.
(6) Official E-mail Address: Provide the user's official e-mail address.
(7) Job Title and Grade/Rank: Provide the civilian job title/grade (Example: Systems Analyst, GS-14; Pay Clerk, GS-5)/military rank (COL, United States Army; CMSgt, USAF) or "CONT" if user is a contractor.
(8) Official Mailing Address: Provide the user's official mailing address.
(9) Citizenship: Select US; it is the only valid option for this block. Other selections will prohibit completion of the request.
(10) Designation of Person: Select Military, Civilian, or Contractor.

User Agreement:

IA Training and Awareness Certification Requirements: User checks the box and provides the date that he/she has completed the Annual Information Awareness Training. The user must have completed this annual training within one year of this access request.

- (11) User Signature: User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).
(12) Date: The date that the user signs the form.

B. PART II: ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR, AND IAO

User's Supervisor or Government Sponsor completes 13 through 20b.

- (13) Justification for Access: Supervisor or Government Sponsor provides a brief statement that is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified. Include the following justification: "Individual identified is a production end-user of the CAMS-ME system. This individual will require access to the CAMS-ME System specified within the "System Name" block, which is located at the beginning of this form. Justification for access will be routed through the CAMS-ME Information Assurance Officer (IAO)."
(14) Type of Access Required: Supervisor or Government Sponsor places an "X" in the appropriate box.
- Authorized - Individual with normal access.
- Privileged - Those with privilege to amend or change system configuration, parameters, or settings.
Place an "X" in the box labeled "Authorized." Do not write anything else in this area.
(15) User Requires Access To: Supervisor or Government Sponsor places an "X" in the appropriate box. Specify category. Place an "X" in the box labeled "Unclassified." Do not write anything else in this area.
(16) Verification of Need to Know: Supervisor or Government Sponsor must check the box, which certifies that the user requires access as requested.
(16a) Access Expiration Date: Supervisor or Government Sponsor specifies expiration date if less than 1 year. Leave blank if block (10) is selected as Military or Civilian. Contractors must include their company name, contract number and contract expiration date.
(17) Supervisor's Name (Print Name): Supervisor or Government Sponsor prints his/her name to indicate that the above information and required training (indicated in Block 27h) have been verified and that access is required.
(18) Supervisor's Signature: Supervisor or Government Sponsor's signature is required by the endorser or his/her representative.
(19) Date: The date the Supervisor or Government Sponsor signs the form. This date cannot precede the date of the user's signature in block 12.
(20) Supervisor's Organization/Department: Supervisor's organization and department.
(20a) Email address: Supervisor or Government Sponsor's email address.
(20b) Phone Number: Supervisor or Government Sponsor's telephone number.
Component Information Owner completes 21 through 21b
(21) Signature of Information Owner/OPR: The specified CAMS-ME Component Information Owner will sign and date block 21.
(21a) Phone Number: Component Information Owner telephone number.
(21b) Date: The date the Component Information Owner signs the DD Form 2875. This date cannot precede the date of the user's signature in block 12.

INSTRUCTIONS FOR THE PRE-POPULATED CAMS-ME PORTAL DD FORM 2875

Information Assurance Officer (IAO) completes 22 through 25

(Follows submission of completed form to the CAMS-ME Help Desk by the Component Information Owner).

(22) Signature of Information Assurance Officer (IAO) or Appointee: The CAMS-ME IAO will sign block 22.

(23) Organization/Department: IAO's organization and department.

(24) Phone Number: IAO's telephone number.

(25) Date: The date IAO signs the DD Form 2875.

(26) User completes 26a and 26b

(26a) Name: Pre-populated from block 1.

(26b) Social Security Number: Pre-populated from block 2.

(27) User's Supervisor or Government Sponsor completes block 27

Block 27 requires a clear and specific explanation as to the access needed and why. The accompanying justification, which immediately follows, is recommended: "Portal access is requested to support the MEV business management objectives. This individual is a Production user of this application."

C. PART III: SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

For government employees, the Security Manager will be the Local Government Security Officer.

For contractor employees, the Security Manager will be either the Local Government Security Officer or the contractor's company security officer.

By completing Part III, to include signing Block 31, the Security Manager is attesting to the validity of the information supplied in Blocks 28, 28a, 28b, and 28c. DoD regulations require a background investigation (at a minimum NAC/NACL) for government and contractor employees.

(28) Type of Investigation: Provide the user's last type of background investigation (i.e., NAC, NACL, or SSBI). The Security Manager will indicate the type of investigation. For government employees a NAC check is the minimally acceptable investigation, while for contractors it is a NACL.

(28a) Date of Investigation: The Security Manager will enter the date of the investigation identified in Block 28.

(28b) Clearance Level: The user's current security clearance level (Secret or Top Secret). The Security Manager will enter the determined clearance from the investigation.

(28c) IT Level Designation: The user's IT designation (Level I, Level II, or Level III). The Security Manager will enter one IT level designation resulting from the investigation.

(29) Verified By: The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Security Manager Telephone Number: The telephone number of the Security Manager or his/her representative.

(31) Security Manager Signature: The Security Manager or his/her representative indicates that the above clearance and investigation information has been verified.

(32) Date: The date that the form was signed by the Security Manager or his/her representative.

PART IV: COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

The "System" block will be pre-populated from the "System Name" block at the beginning (above Part I) of this form.

D. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system. User should deliver the form to his/her Supervisor or Government Sponsor, who must complete and sign blocks 13 through 20b and block 27; obtain completion of Part III from the Security Manager; and then deliver the form (including Part II supplement and signature page, J-5, of System Rules of Behavior) to the Component Information Owner. Component Information Owner must complete and sign blocks 21 through 21b and deliver the form (including the signature page, J-5, of the System Rules of Behavior) to the CAMS-ME Help Desk to complete the process.

F. Instructions for DD FORM 2875 PART II Continuation of Block 27 FOR CAMS-ME Use. To be completed by User.

All grayed out areas are not applicable for CAMS-ME GUI Users.

(27a) System(s): If you are completing this form as a CAMS-ME Portal User or CAMS-ME GUI User, select CAMS-ME.

(27b) and (27c) Leave blank.

(27d) Application: Select the appropriate user access option.

(27e) through (27g) Leave blank.

(27h) Complete for all access requests: You must supply all requested information. Below are instructions for locating your EDI Personal Identifier. Also, all CAMS-ME Portal users and all CAMS-ME GUI users requesting access must have completed the identified training before requesting access to CAMS-ME.

EDI Personal Identifier Instructions:

- i. Open Internet Explorer / select Tools from toolbar / select Internet Options.
ii. Select Content tab / select Certificates / select Personal tab.
iii. Select your Class 3 certificate by double-clicking it.
iv. Select Details tab / select Field labeled "subject."
v. You will see an item marked as "CN =" followed by your LAST NAME. FIRST NAME. MIDDLE INITIAL. 10 digit numeric field. This 10-digit field is your EDI Personal identifier.

(27i) Leave blank.

(27j) For Modified Part II Only (Complete Only for Changes): This block is to be completed when requesting a change to an already processed access request. You are required to complete an updated DD Form 2875 Part II supplement and must include all required signatures and dates in block 27j (User's, Supervisor's or Government Sponsor's, and designated Component Information Owner, who is also the FIO).

(27k) Please select the appropriate user profile. You may only select ONE profile. This selection must agree with the Component Agency identified in block 27h as well as the application(s) or module(s) selected in block 27d.

**STANDARD MANDATORY NOTICE AND CONSENT PROVISION
FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS
(STANDARD AGREEMENT TRAINING)**

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 counter-intelligence (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 the 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.

System Security Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training

All Users shall:

- Hold US Government security clearances and have completed background checks commensurate with the level of information to which they are being granted access.
- Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only those roles and privileges for which they are authorized.
- Protect information and system resources against occurrences of sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse or release to unauthorized persons. Immediately report all such occurrences described above to their Information Assurance Manager (IAM).
- Follow current DoD password (PW) configuration rules mandated by Joint Task Force - Global Network Operations (JTF-GNO), when a User ID and PW are required to access a system.
- Protect their password(s) and/or Common Access Card (CAC) personal identification number (PIN). Promptly change their password/PIN when possibly compromised, forgotten or when it appears in an audit document. Immediately notify their Terminal Area Security Officer (TASO) or their IAM if they believe their password/PIN has been compromised and promptly change their password/PIN. (Your TASO or IAM will verify that your password changed and/or PIN has been reset.)
- Ensure that system media and output are properly marked, controlled, stored, transported, and destroyed based on classification or sensitivity and need-to-know.
- Ensure all documents, equipment, and machine-readable media containing sensitive data are cleared, properly marked, and sanitized before being released outside of the Department of Defense. Contractors shall ensure documents, equipment, and machine-readable media containing sensitive data are cleared, properly marked, and sanitized before these items are used to support another contract. (See DoD 5200.1-R, Information Security Program for releasing documents outside of DoD.)
- Protect terminals or workstations from unauthorized access. Remove their CAC from the reader when leaving their workstation. If the workstation has not been CAC-enabled, lock it before leaving. Also, activate the desktop screen saver and set the idle time out period to 15 minutes. Contact the Service Desk for assistance in locking the workstation and activating the screen saver.
- Ensure that devices that display or output sensitive information in human-readable form are positioned to deter unauthorized individuals from reading the information and/or obtain a Privacy screen filter for your monitor.
- Inform the supervisor when access to a particular DoD information system or enclave is no longer required (e.g., completion of project, transfer, retirement, and resignation).
- Observe rules and regulations governing the secure operation and authorized use of a DoD information system or enclave; Use the DoD information system or enclave only for authorized purposes; Not introduce malicious code into any DoD information system or enclave or physically damage the system or enclave.

- Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed; users shall coordinate the procedure with the IAM and receive written approval.
- Not introduce or use unauthorized software, firmware, or hardware onto the DoD information system or enclave.
- Not relocate or change DoD information system or enclave equipment or the network connectivity of equipment without proper IA authorization.
- Not use wireless enabled equipment while physically connected to the system
- Understand that system use constitutes consent to monitoring, recording and auditing.
- Comply with Business Transformation Agency's Information Technology policies as they appear in the current version of IT Instruction 7400.

Additionally, Administrative and Privileged users shall:

- Utilize public key (PK)-enabled government owned or controlled computers that have wireless computing capabilities disabled.
- Connect to the system using FIPS 140-2 validated virtual private network (VPN) software when authorized to work remotely.
- Follow current DoD password (PW) configuration rules mandated by Joint Task Force - Global Network Operations (JTF-GNO), when a User ID and PW are required to access a system.

Exceptions granted by an Information Assurance Officer or an Information Assurance Manager to any of the above rules shall be confirmed in writing and provided to the Deputy Designated Accrediting Authority (DAA) for the Business Transformation Agency.

If you have any questions or comments about the information presented here, please contact the Service Desk.

CAMS-ME System Specific Security Rules of Behavior

1. Users are not permitted multiple logon sessions.
2. Users shall comply with Portal Logon and GUI Logon Procedures, provided by the Columbus Call Center at the time initial access is granted.
3. Out-of-Band (OOB) users shall comply with the DISA Computing Services Instruction 100-55-21, January 12, 2004 and the CAMS-ME 1.1 OOB Access Justification & Authorized Users Policy, February 21, 2006.
4. Users shall ensure that all workstations and mobile computing devices implement virus protection that is kept up-to-date.
5. Users shall ensure that data/information is never loaded or stored on a workstation, a laptop or any type of storage device.
6. Users working at a non-government facility shall ensure that workstations and/or laptops are secured and locked at all times.
7. Users in possession of a PKI Class 3 soft certificate shall ensure that they appeared in person before the certifying authority when applying for their certificate.
8. Users working from home shall ensure compliance with their agency's work-at-home policy.
9. Users employing wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices shall ensure implementation in accordance with DoD wireless policy, as issued.

Privacy Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training

- You may be granted access to personal information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., social security number, age, rank/grade, marital status, race, salary, medical information or complete personal bank account number, etc. Such information is also known as personally identifiable information (PII).
- The computer screen where personally identifiable information appears must be labeled with “For Official Use Only” Privacy Act of 1974, As amended.” If the system cannot be changed to have this appear on each screen, it must be on the log-in screen to the system, or a Privacy label may be placed on the computer monitor. The Privacy label shall read, “Personal Data, Privacy Act of 1974, as Amended, 5 U.S.C. 522a.
- Printed output products must be properly labeled with "For Official Use Only” “Privacy Act of 1974, As amended.” The policy for labeling output products containing Privacy Act information is in DoD 5200.1-R, Appendix 3, page 141 and DoD 5400.11-R, paragraph C1.4.
- Place the standard Privacy Act warning label on the top of your computer monitor if names and social security numbers/personal bank account numbers, etc., are on your computer screen while you do your work. These labels can be generated on a plain white label that must read: “Personal Data, Privacy Act of 1974, as Amended, 5 U.S.C. 552a.”
- PII in DoD systems must be protected from unauthorized access especially when the system is in use and when the information is printed. The Privacy Act of 1974, As amended, 5 U.S.C. § 552a(i) also provides for criminal penalties.
 - (1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain personally identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.
 - (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e) (4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.
 - (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses may be found guilty in a court of law of a misdemeanor and fined not more than \$5,000.
- If you have any questions or comments about the information presented here, please contact the Service Desk.

User's Acknowledgement of Standard Agreement, Security and Privacy Training

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

I have read and consent to the terms in the Standard Mandatory Notice & Consent Provision For All DoD Information System User Agreements (Standard Agreement Training).

I have read and consent to the terms in the System Security Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.

I have read and consent to the terms in the Privacy Rules of Behavior (ROB)/Acceptable Use Policy (AUP) Training.

I also agree to follow the standard agreement and these rules as a condition of being granted system access.

(Check the applicable items, print your full name, sign, date and print your DoD Component and office)

Standard Agreement Training	Yes <input type="checkbox"/>
System Security ROB/AUP Training	Yes <input type="checkbox"/>
CAMS-ME System Specific Security ROB	Yes <input type="checkbox"/>
Privacy ROB/AUP Training	Yes <input type="checkbox"/>

Print Full Name (Last, First, Middle) _____

Signature _____ Date _____

DoD Component/Office _____

Attach this completed page to the DD Form 2875 at the time Part I is completed.