***Maintenance, Overhaul and/or Upgrade* Requirements**

I. INTRODUCTION

A. Army Materiel Command (AMC) and its units use Total Asset Visibility – Contractor (TAV-C) capability in its Logistics Management Program (LMP) to account for Government Furnished Equipment, Materiel, or Property (GFE/M/P) placed in the possession of contractors to support contracts for: 1) Maintenance, overhaul, or upgrade work; 2) materials held for Stock, Store and Issue (SSI), or 3) New Production. Accounting records within LMP for this inventory are subject to verifying physical inventories and audits by the Army to ensure accuracy. This section addresses contractor requirements for maintenance, overhaul and/or upgrade contracts.

II. SYSTEM OVERVIEW AND PORTAL ACCESS REQUIREMENTS

A. To use TAV-C, Contractors shall request one of two TAV-C access methods below to exchange required inventory data with LMP: 1) Defense Logistics Management Standards (DLMS) interface or 2) the Army TAV-C Portal. Approval of the contractor's access method will be based first on the type of work being performed, second, the sufficiency of the contractor's existing property accountability and connectivity to LMP, and third, request by the contractor to use the portal based on economic factors.

B. Contractors shall choose between the two methods for accounting for Government property as further described below:

1. DLMS interfaces: Contractors that have accounting systems capable of using a DLMS interface (see: DLM 4000.25, Defense Logistics Management Standards (DLMS) on the Defense Logistics Agency (DLA) website https://www.dla.mil/) shall request to use their accounting system and interface to account for GFE/M/P using DLMS transactions.

NOTE: If a contractor does not currently have an established DLMS interchange with DLA Defense Automated Addressing System (DAAS), the Contractor shall contact DAAS to establish access to DAAS messaging system to support the exchange of DLMS transactions with the Army. DAAS provides a value added service for standard Military Standards (MILS) transactions providing the ability to receive, edit and route logistics transactions for the Military Services and Federal Agencies. Information on DAAS can be found at https://www.dla.mil/HQ/InformationOperations/DAAS/

2. Army TAV-C Portal: Contractors, who, during negotiation with the Government, are determined to be allowed to use the TAV-C Portal, shall comply with prescribed processes to provide qualified workers to access the system to exchange data with LMP.

C. Portal Access Requirements. Contractor personnel, who input data into the TAV-C Portal, shall meet qualification requirements specified in the TAV-C Portal User Access – End User SOP. These requirements include:

1. Contractor provided computer system: The contractor shall provide a computer system and internet connectivity that meets acceptable standards as identified in the TAV-C Portal User Access – End User SOP.

2. Security Requirements.

(a) The Government requires contractor personnel accessing the LMP system to possess either a United States Government Common Access Card (CAC) or a

Department of the Defense approved ICAM Multi-Factor Authentication (MFA) Certificate.

NOTE: It is the contractors' responsibility ensure operators accessing the portal have and maintain current credential and to comply with contract requirements.

(b) Contractors will coordinate with the Contracting Officer's Representative (COR) or designated government sponsor (herein referred to sponsor) to complete required online access registration and MFA process.

3. User Training Requirements: TAV-C Portal user training is Government provided and varies by the function performed. The training is online and completion of the training by each operator is required before accessing and using TAV-C.

4. The on-line training site will be provided by the government after award and access to the system has been granted. Functional training required to begin work should take approximately 1 hour to complete. The following courses are required for contractor overhaul and are listed under the TAV-C Portal User Role to Training Course Matrix section in the TAV-C Portal User Access – End User SOP.

    a. LMP_TAVC_EDU_109_WBT

    b. LMP_TAVC_DIST_204_WBT

D. Problem Resolution: LMP is a Government owned and maintained system. The contractor shall notify the COR or designated Government point of contact for system related issues and Government resolution.

III. DLMS TRANSACTIONS / PORTAL DATA REQUIREMENTS

A. For maintenance, overhaul and/or upgrade contracts, the contractor shall provide inventory management transactions to the Government by DLMS interface as follows:

1. DLMS 527R Materiel Receipt Acknowledgement (MRA) Transactions (for Government Furnished Material (GFM) expected to be consumed and GFE-R carcasses provided for overhaul).

B. For DLMS Transactions for maintenance, overhaul, and/or upgrade contracts, the material receipt transactions to be provided to the contractor by the Government via the DLMS interface are:

1. DLMS 527D Pre-positioned Material Receipt Document for stock in-transit to vendor.

C. Army TAV-C Portal: Contractors who, during negotiation with the Government, are allowed to use the TAV-C Portal shall exchange required data directly with LMP. Contractors who use the TAV-C Portal shall provide the following information via data inputs to LMP.

1. TAV-C Portal Requirements: Material Receipt Acknowledgment (MRA)

IV. PERFORMANCE REQUIREMENTS

A. The Contractor shall physically confirm material received (MRA) for actual National Item Identification Number (NIIN) and Quantity prior to recording receipt into LMP through DLMS or the TAV-C Portal.

Logistics Modernization Program
Total Asset Visibility – Contractor (TAV-C)
Portal Access Standard Operating Procedure for End Users (version 05)

Change: User access procedures have been updated; SOP separated by role; added detail regarding annual IA training requirements

LMP's TAV-C capability extends asset visibility to contractor locations, contributes to bettering the Army's view of assets, and supports Army Readiness.

March 2023

Table of Contents

Introduction **3**
Purpose Statement **3**
TAV-C Portal Access – ICAM Account Process Flow **4**
General Process Information & Assumptions **4**
Process Details – Performed by the End User (without a CAC) **5**
Process Details – End User with CAC **6**
TAV-C Portal User Role to Training Course Matrix **8**
Terms & Acronym List **8**
Appendix A – End User Instructions **9**
Create an Identity Record in (AMID) ***9***
Multi-Factor Authentication ***14***
HELPFUL LINKS & RESOURCES **16**

Introduction

Logistics Modernization Program's (LMP) Total Asset Visibility – Contractor (TAV-C) capability was developed to resolve audit findings related to the management of Army property. TAV-C capability extends asset visibility into contractor locations through improved recordkeeping and provides more accurate reports associated with this Government property. Use of TAV-C functionality by contractors is mandatory for Army Working Capital Fund (AWCF) managed property in the possession of contractors. This solution contributes to the management of assets supporting global equipment Readiness through LMP.

Contractors using the TAV-C Portal to input information into LMP will comply with the access processes described in this guide to establish and maintain user accounts, complete access processes, as well as Department of Defense (DoD) approved authentication, to receive access to this capability. The approved authentication is achieved one of two ways: with a Common Access Card (CAC) or via the creation of an Identity, Credential, and Access Management (ICAM) account in conjunction with multi-factor authentication. The ICAM program is designed to provide the mechanism for external entities to securely communicate with the DoD and authenticate to DoD information systems.

It is recommended Contractors carefully review this document and consider the amount of time needed to establish and maintain user security credentials, complete mandatory systems access training, apply for access to the system, and complete task specific user training.

— Until these requirements are satisfied, portal access will not be granted. —

The Training to FSR Matrix provides a list of user functional training courses and refer to the solicitation to verify the TAV-C functions needed for the effort.

Purpose Statement

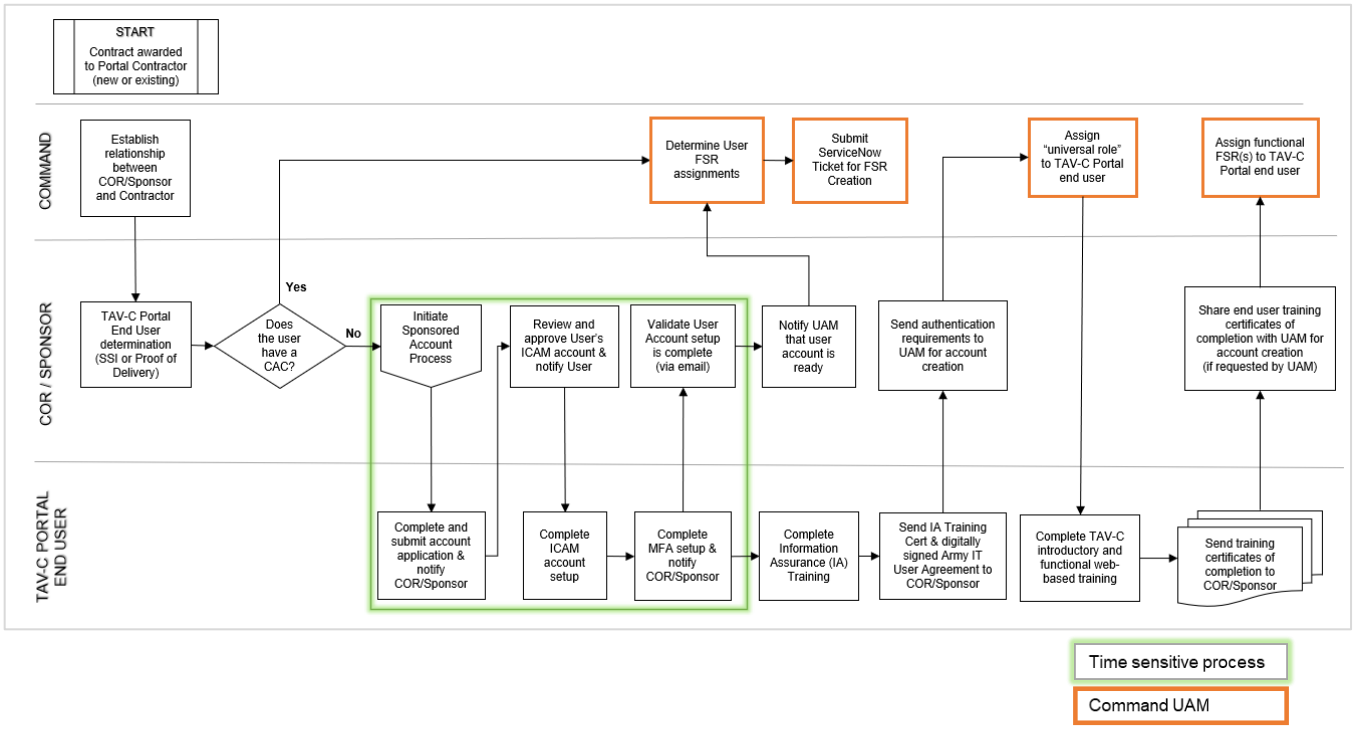
The purpose of this document is to provide an understanding of the process for gaining access to the LMP TAV-C Portal solution for TAV-C Portal Contractors. The TAV-C Portal Contractors include:

1) Stock, Store, and Issue Contractor Portal Users
2) Vendor Proof of Delivery Contractor Portal Users

Please note that the DoD ICAM process illustrated in this document provide instructions on how to request an account and register in through Army Mobile Connect on any device that allows the user to get to the app store for double authentication. (Cellular phone or tablet) etc. Apple Store, Google Store or TRADOC App Gateway.

Internet Access to the LMP TAV-C Portal has been validated using Windows 10 or later, Edge, and Google Chrome browsers. Hardware requirements for LMP TAV-C Portal would be any hardware that can support Windows 10, Edge, and Google Chrome and connect to the Internet.

TAV-C Portal Access – ICAM Account Process Flow



General Process Information & Assumptions

- In accordance with AMC Operations Order 19-229, dated 111810Z Sep 2019, this guide establishes procedures and guidance for users to gain access to the TAV-C Portal.
- The Contracting Officer (KO) works with the requiring activity to establish a Contract Officer's Representative (COR) (preferrable) to appoint for contract users. If the contract has no COR, the requiring activity shall immediately appoint a DA Civilian to serve as sponsor. The COR/DA Civilian is referred to as the sponsor hereafter.
- The sponsor informs the TAV-C Portal contractor of these procedures and requirements and assists end users with gaining access to the TAV-C Portal. The sponsor reviews and approves the establishment of LMP end user accounts supporting TAV-C Portal processes. The sponsor functions as the Contractor's point of contact for LMP systems issues.
- The Sponsor works with the designated Command UAM Administrator to identify TAV-C Portal Functional Security Roles (FSRs) required by the contractor.
- Organizations will follow their documented policy for assigning FSR to Portal end users.
- The COR/Sponsor works with the designated Command UAM Administrator to identify the access required by the contractor.
- The Command UAM will manage the required annual account review, which is required for TAV-C Portal end users.

Process Details – Performed by the End User (without a CAC)

TAV-C Portal users who will not be using a CAC are required to have the following:

- Signed memorandum from the Company stating that the User is an employee of the company and confirm U.S. Citizenship status
- Identify, Credential, and Access Management (ICAM) account
- Identity record in Army Master Identity Directory (AMID)
- Multi-factor authentication (MFA)

The information in this section is for TAV-C users without a CAC. Proceed to the Process Details - Performed by the End User (with CAC) section for CAC-enabled user guidance. The End User will be contacted by the COR/Sponsor to begin the ICAM account creation process. The ICAM account process will result in the User having an account setup in AMID. This is a time-sensitive process. See Appendix A for step-by-step instructions. The End User process steps are as follows:

1. User receives an email application to create their account in AMID via the ICAM Portal.
2. User completes the application information and submits the application, then notifies the Sponsor.
3. User receives a confirmation e-mail that their application has been approved by the Sponsor.
4. User completes the ICAM account setup process, which includes setting a password and setting up security questions.
5. User verifies they can log into the ICAM Portal successfully with their username and password.
6. User sets up multi-factor authentication (MFA) and notifies the Sponsor that their account creation and MFA setup is complete.
7. Non-CAC Users will complete the following requirements:
    a. **Information Assurance/Cyber Awareness (IA/CA) Training** for Non-CAC enabled users @ https://public.cyber.mil/ → Training → Cyber Awareness Challenge.
    b. **Mandated Army IT User Agreement** → the non-CAC user will receive a blank copy of the IT User Agreement to complete and print their full name and sign (with blue or black ink).
    c. Non-CAC holder will take the IA training and sign the Army IT User Agreement **every year**.
8. Once #7 is complete, the User sends the IA Training certificate and signed Army IT User Agreement to their Contracting Officer (KO), COR or Sponsor; these requirements must be completed before submitting any access requests.
    a. The Army IT User Agreement will be re-signed annually, and the IA Training will be completed annually.

b. The Army IT User Agreement and IA Training will also be repeated if assigned to another contract. The current Army IT User Agreement is not allowed to roll-over to a new contract.

9. The COR/Sponsor and UAM will continue the process and grant the user the "TAV-C Universal Role" to allow the User access to the TAV-C Training Library via the TAV-C Portal

   a. Users must complete appropriate TAV-C functional web-based training courses. See TAV-C Portal User Role to Training Course Matrix for further guidance.

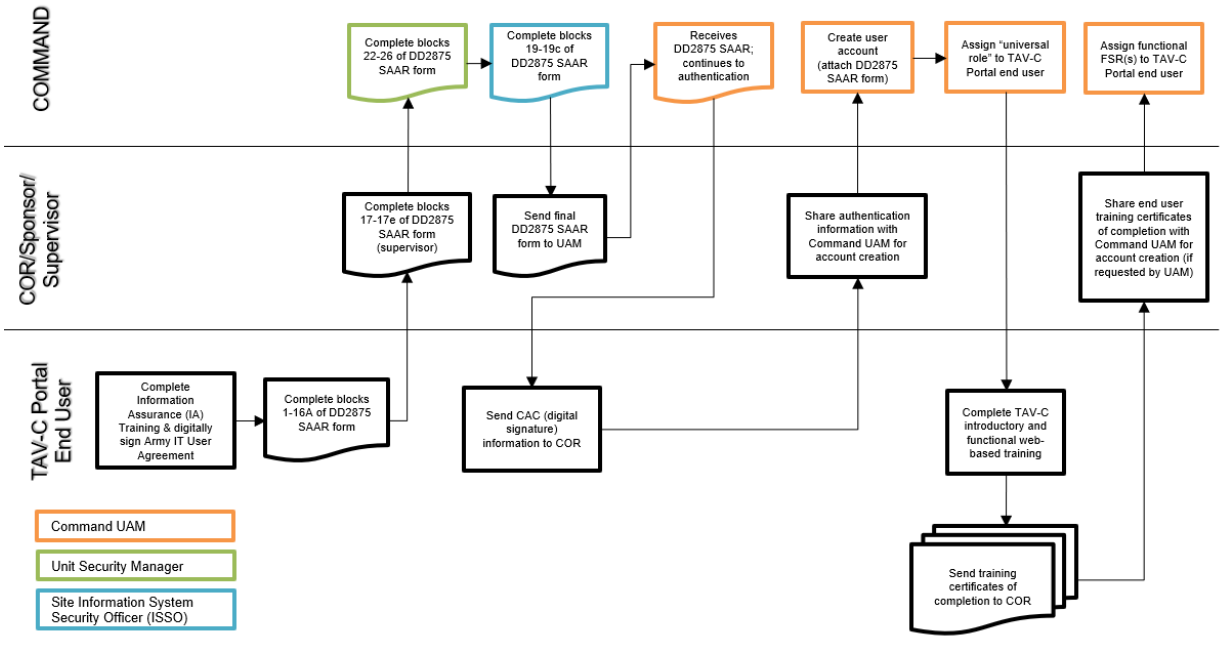
   b. User will send their TAV-C training certifications to their COR/Sponsor to be sent to the UAM for final LMP functional security role (FSR) access provisions.

10. Once LMP account is updated and FSRs are assigned, the User can begin using the TAV-C Portal with their ICAM Account Username, Password and MFA.

Process Details – End User with CAC

TAV-C Portal Users who will be getting a CAC, or who have a CAC, should work with their designated UAM for guidance on getting an LMP account. This is an existing process. A signed company memo is still recommended for TAV-C CAC users, if they will only be using LMP for TAV-C purposes.

For initial guidance, refer to the process flow and steps below.



The steps below are needed to complete a System Authorization Access Request (SAAR) to grant LMP access. This is for CAC users only. NOTE: The SAAR form is subject to change; this is based off the form as of May 2022.

- **TAV-C Portal CAC end user** completes blocks 1 through 16A of the of DD 2875 and submit to user UAM.

- **Supervisor for CAC holders** completes blocks 17-17e of the DD 2875 and submits to responsible Unit Security Manager.
- **Unit Security Manager** completes blocks 22-26 of DD 2875 & and return to requester.
- **Site Information System Security Officer (ISSO)** completes blocks 19 – 19c of DD 2875 and returns to the requester.
- **Site UAMs** receive the completed SAAR form and add it to the user's LMP account once the account is created.

Please note that the following requirements will be completed annually:

1. Complete the Information Assurance/Cyber Awareness (IA/CA) Training @ https://cs.signal.army.mil/ → Click on the link to **Cyber Awareness Training** (CAC login required)
2. Digitally signed Army IT User Agreement @ https://cs.signal.army.mil/ → Click on the link to the **Mandated Army IT User Agreement** (CAC login required)

TAV-C Portal User Role to Training Course Matrix

Training Course ID	Training Course Title	Audience	FSR UAM Tech Name(s)
LMP_TAVC_EDU_109_WBT	TAV-C Portal - SSI Contractor Overview	All Portal SSI Contractors	N/A
LMP_TAVC_IMWM_316_WBT	TAV-C Portal - Cycle Count Leader	SSI Contractors - Cycle Count Leaders	QRF-IMWM00000071
LMP_TAVC_IMWM_317_WBT	TAV-C Portal - Cycle Count Manager	SSI Contractors - Cycle Count Managers	QRF-IMWM00000070
LMP_TAVC_IMWM_319_WBT	TAV-C Portal - Receiving Specialist	SSI Contractors - Receiving Specialists	QRF-IMWM00000072
LMP_TAVC_IMWM_318_WBT	TAV-C Portal - Inventory Processor	SSI Contractors - Inventory Processors	QRF-IMWM00000069
LMP_TAVC_DIST_323_WBT	TAV-C Portal - Delivery Processor	SSI Contractors - Delivery Processors	QRF-IMWM00000063
LMP_TAVC_DIST_324_WBT	TAV-C Portal - Denial Processor	SSI Contractors - Denial Processors	QRF-IMWM00000065
LMP_TAVC_DIST_325_WBT	TAV-C Portal - Cancellation Processor	SSI Contractors - Cancellation Processors	QRF-IMWM00000066
LMP_TAVC_DIST_326_WBT	TAV-C Portal - Ship-in-Place Processor	SSI Contractors - Ship in Place Delivery Processors	QRF-IMWM00000067
LMP_TAVC_IWMW_320_WBT	TAV-C Portal - Reports	SSI Contractors - Reporting	URF-ALL-00000004
LMP_TAVC_DIST_204_WBT	TAV-C Portal - Vendor/Contractor Proof of Delivery	All Vendor/Contractors using Portal Proof of Delivery	QRF-DIST00000064 QRF-DIST00000069

Terms & Acronym List

Acronym	Name
ACC	Army Contracting Command
AMC	Army Materiel Command
AMID	Army Master Identity Directory
CA	Cyber Awareness
CAC	Common Access Card
DoD	Department of Defense
FSR	Functional Security Roles
HQ	Headquarters
IA	Information Assurance
ICAM	Identity, Credential, Access Management
SAAR	System Authorization Access Request
SPONSOR	Contracting Officer's Representative or Government Sponsor
TAV-C	Total Asset Visibility – Contractor
UAM	User Account Manager

Appendix A – End User Instructions

Create an Identity Record in (AMID)

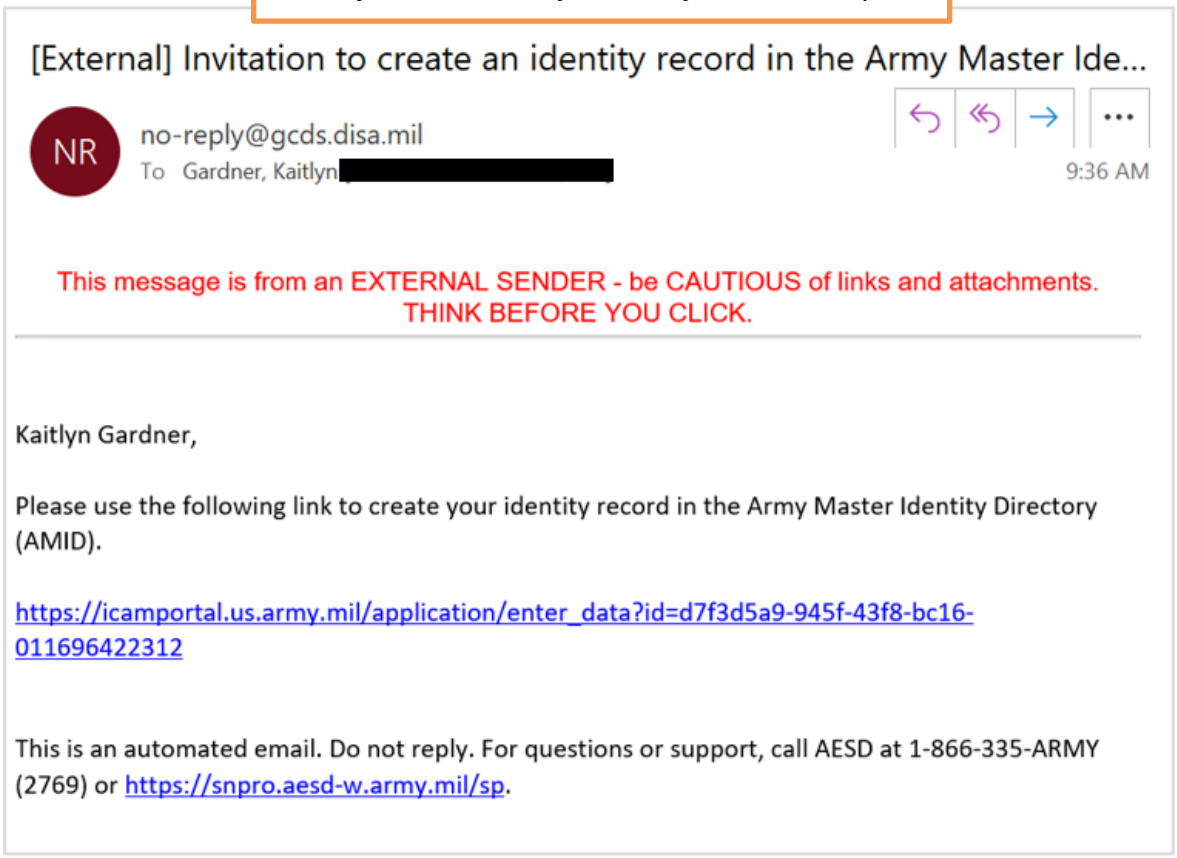
Once the Sponsor has successfully created your sponsored account, you will receive an e-mail to the e-mail address provided during account creation (personal or work e-mail). This will initiate the user's application to create their identity record in Army Master Identity Directory (AMID).

1. Open the email invitation, then copy and paste the link provided in the email into your browser.

NOTE: Launching the link directly from the email may not work depending on your browser, email and security settings therefore it is recommended you copy and paste the link into the browser manually. If you still get an error using the link, try launching in private or incognito browsing mode.

IMPORTANT: This link expires in 24 hours from the time it was generated; if this link expires, the Sponsor will need to resend it. Therefore, the sponsor shall immediately contact the Invited User by phone or other means to inform them to take immediate action to create an identity account.

Army Master Identity Directory Email Example



[External] Invitation to create an identity record in the Army Master Ide...

NR no-reply@gcds.disa.mil

To Gardner, Kaitlyn[redacted] 9:36 AM

This message is from an EXTERNAL SENDER - be CAUTIOUS of links and attachments.
THINK BEFORE YOU CLICK.

Kaitlyn Gardner,

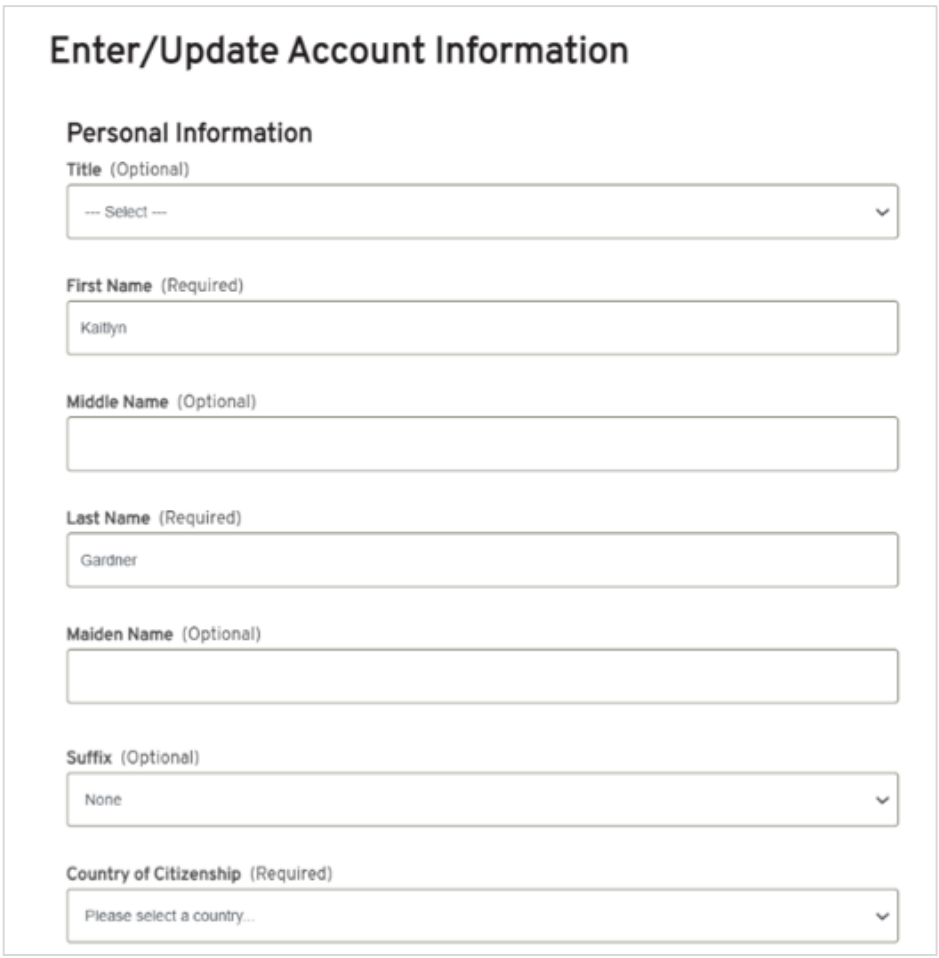
Please use the following link to create your identity record in the Army Master Identity Directory (AMID).

https://icamportal.us.army.mil/application/enter_data?id=d7f3d5a9-945f-43f8-bc16-011696422312

This is an automated email. Do not reply. For questions or support, call AESD at 1-866-335-ARMY (2769) or https://snpro.aesd-w.army.mil/sp.

Appendix A Cont'd

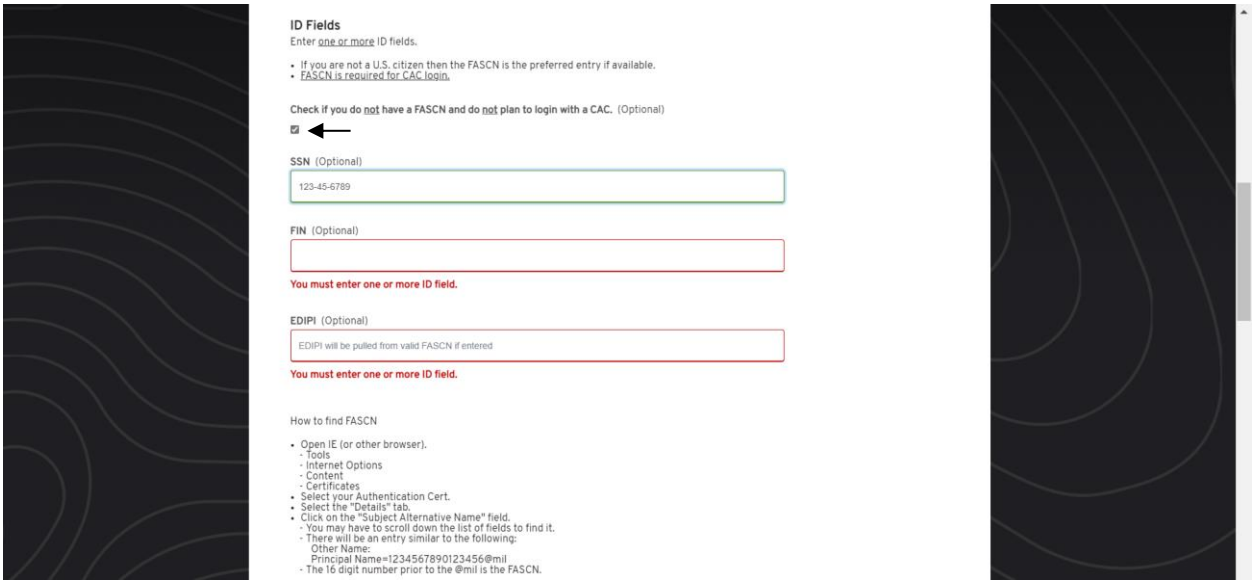
2. Complete the "Personal Information" fields on the "Enter/Update Account Information" page:



Field	Entry	Additional Guidance
Title (Optional)	Enter a title or leave blank	-
First Name (Required)	Enter your first name	-
Middle Name (Optional)	Enter your middle name or leave blank	-
Last Name (Required)	Enter your last name	-
Maiden Name (Optional)	Enter your maiden name or leave blank	-
Suffix (Optional)	Enter a suffix or leave blank	-
Country of Citizenship (Required)	USA	-

Appendix A Cont'd

3. In the "ID Fields" section, **select the checkbox** for *Check if you do not have a FASCN and do not plan to login with a CAC (Optional).* This will populate additional ID fields. Complete the fields:

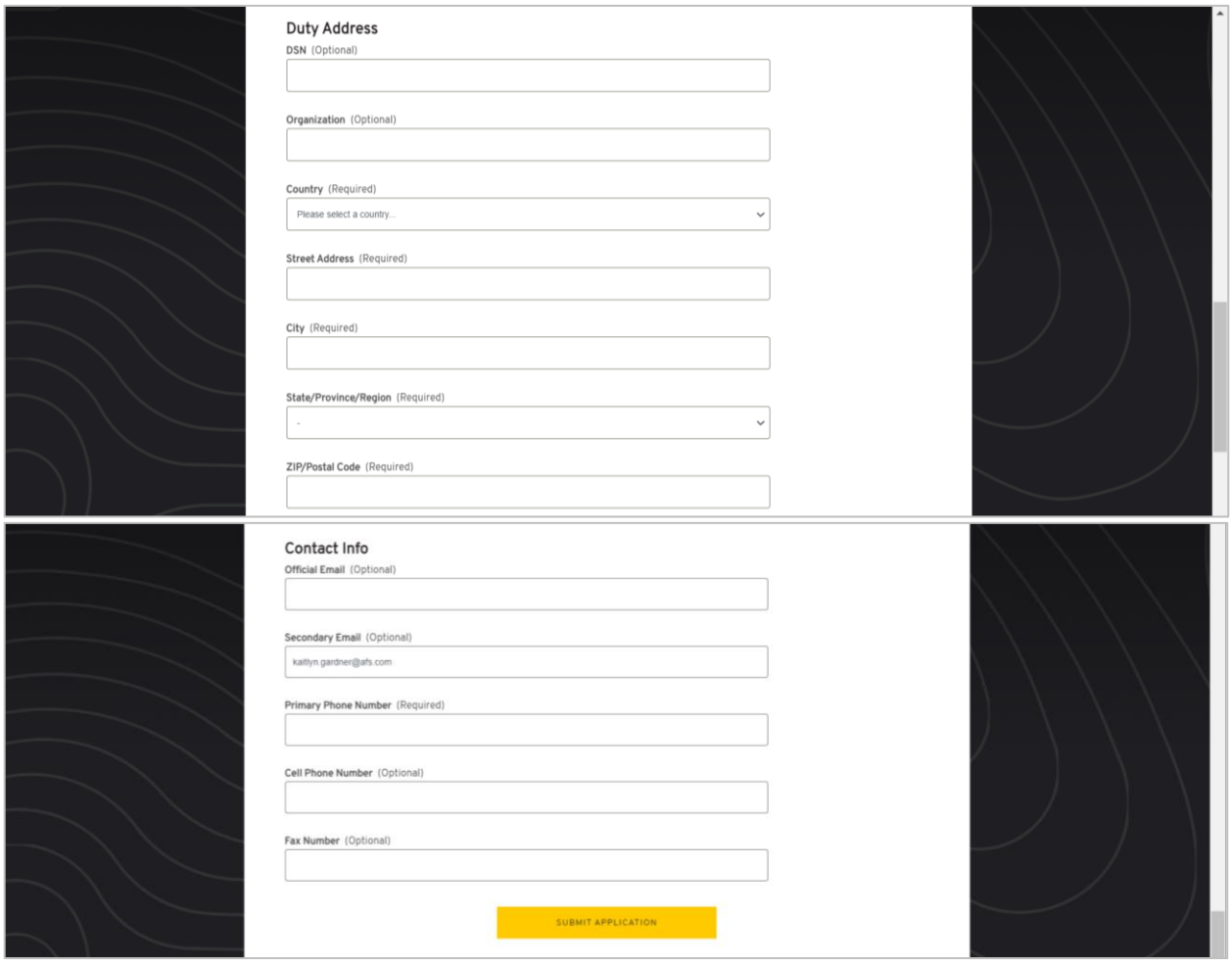


NOTE: You must complete AT LEAST one of the ID fields to be able to submit the application.

Field	Entry	Additional Guidance
SSN (Optional)	Enter your social security number (###-##-####)	- **This is the ONLY valid entry for non-CAC TAV-C end users** - System will validate unique SSN entries and will not accept duplicates; must be in the correct format
FIN (Optional)	Enter a foreign identification number (must be 9 or 10 digits)	- **DO NOT USE: not applicable to LMP TAV-C users** - Duplicate entries are acceptable
EDIPI (Optional)	Blank	- **DO NOT USE: for CAC users only** - User should not have (or use) the EDIPI field

Appendix A Cont'd

4. Complete the "Duty Address" and "Contact Info" fields:

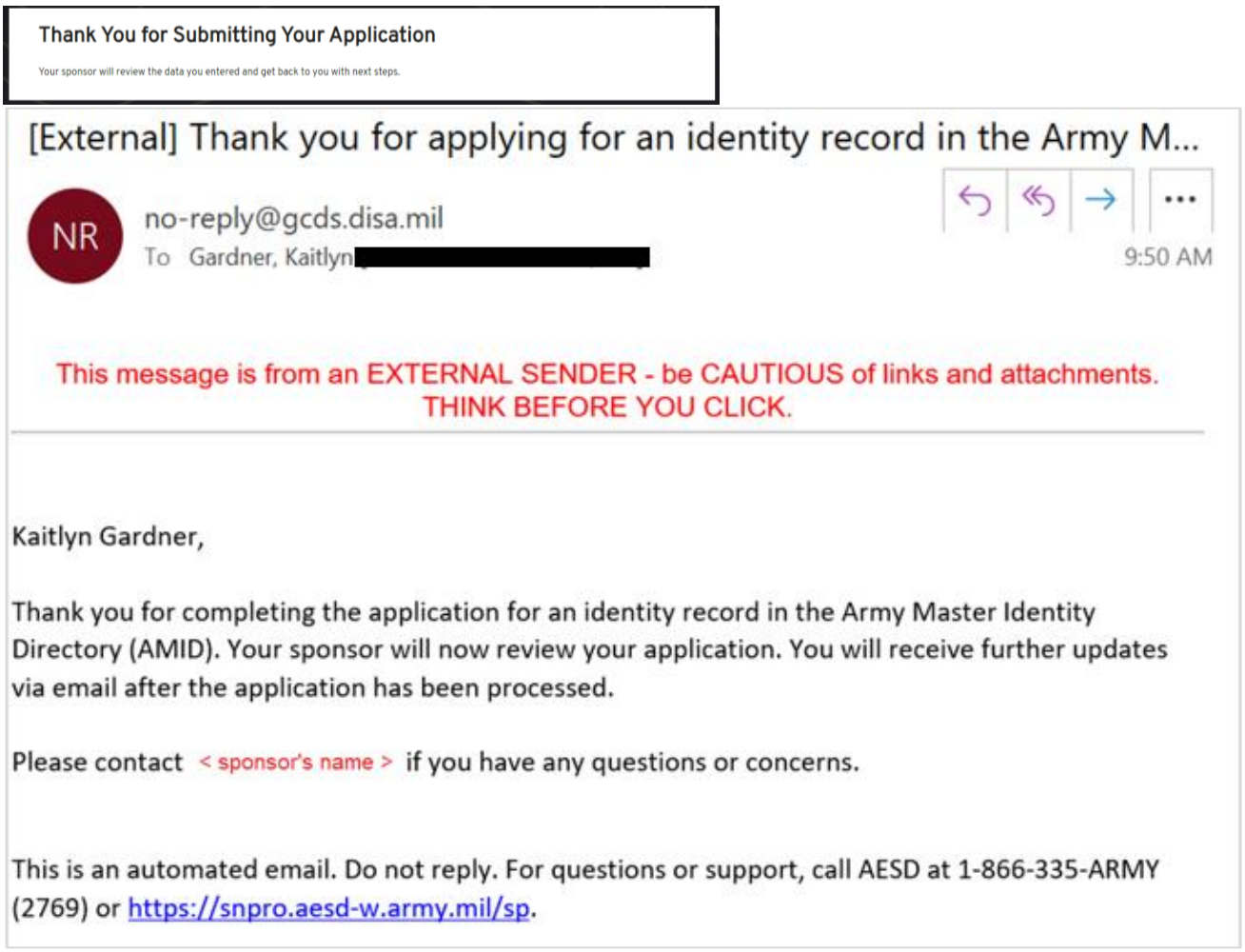


Field	Entry	Additional Guidance
DSN (Optional)	Blank	-
Organization (Optional)	Enter your company name or leave blank	-
Country (Required)	USA	-
Street Address (Required)	Enter your work street address	-
City (Required)	Enter your work city	-
State/Province/Region (Required)	Enter your work state	-
ZIP/Postal Code (Required)	Enter your work zip/postal code	-
Official Email (Optional)	Blank	At least ONE email address is required; use the SECONDARY email field (it should match the email used during account creation)
Secondary Email (Optional)	Enter your personal/work email	

Primary Phone Number (Required)	Enter your phone number	-
Cell Phone Number (Optional)	Enter your cell or leave blank	-
Fax Number (Optional)	Enter a fax or leave blank	-

Appendix A Cont'd

5. Click **SUBMIT APPLICATION.**



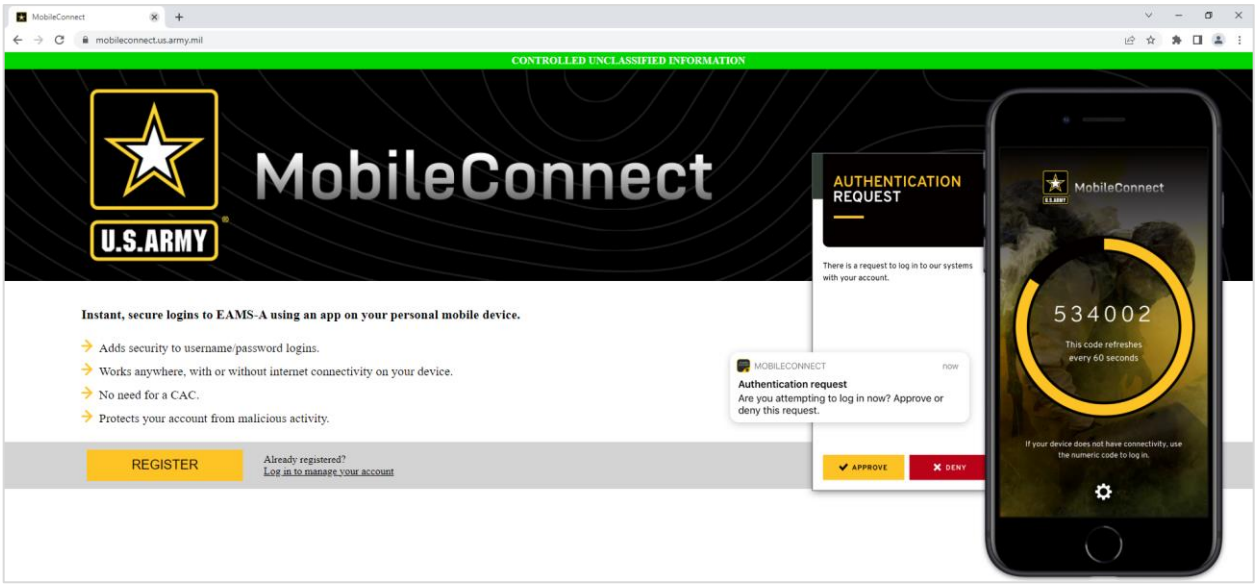
6. You will receive a Thank You confirmation system message and a confirmation email. Notify the Sponsor that the application is complete so they can complete the application approval.

Multi-Factor Authentication

The use of multi-factor authentication is a requirement to access the TAV-C Portal without a CAC. You will require a personal device with access to download apps from the Apple App Store or Google Play.

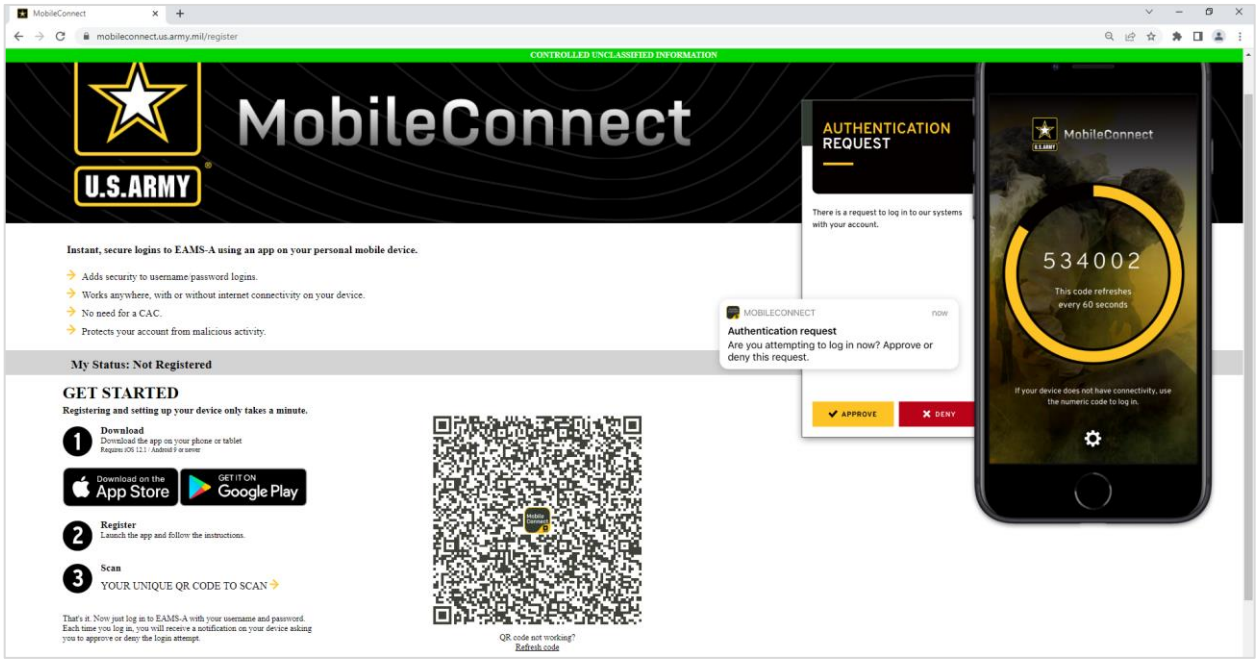
1. Go to the Welcome // ICAM Portal (army.mil) and click on **MobileConnect.**

2. Click **Register.**



3. On the *EAMS-A Login Single Sign-On* page, enter your account username and password and click **Login**.
4. The page will show My Status: Not Registered. Follow the instructions on this page:

a. Download the **MobileConnect** app on the Apple App Store or Google Play.
b. Launch the app and follow the app instructions to register.
c. Scan the unique QR code on this webpage to complete registration. If needed, you can Refresh code from this webpage to update the unique QR code.



5. That's it. Now just log in to EAMS-A with your username and password. Each time you log in, you will receive a notification on your device asking you to approve or deny the login attempt. Be sure to have your device with **MobileConnect** installed handy during login.

HELPFUL LINKS & RESOURCES

Helpful Links

- Welcome // ICAM Portal (army.mil)
- ICAM Portal FAQs (army.mil)
- MobileConnect (army.mil)
- Service Portal - Service Portal (army.mil)

ICAM / EAMS-A Documentation

1. Service Portal - Service Portal (army.mil)
2. Click on **Knowledge**
3. Enter any of the KBA numbers below into the SEARCH field
   - KB0012454 - ICAM: Account Types & Sponsorship
   - KB0012455 - ICAM: How to Initiate Sponsorship
   - KB0012656 - ICAM: How to Transfer a Guest to Another Sponsor
   - KB0012451 - How to Reset your Password

Help Desk

- Contact AESD at 1-866-335-ARMY (2769) - for EAMS-A, ICAM, MFA