# ALERTS Training Accounts

Training is an integral part of keeping our forces up to date on regulations, policies, and procedures that effect our current and future operational environments across the entire spectrum as a 21st century Warrior. Academic learning should continue past the schoolhouse environment with on the job and situational training at the Soldier and unit level. This will encourage a reinforcement of lessons and ideas taught in core curriculums at U.S. Army schools.

Additionally, training accounts on web-based systems and databases should be initialized and created at the Initial Entry Training for Soldiers. These accounts should be maintained by local and installation level training officers and administrators once the students have graduated. This allows Soldiers to be life-long learners as well as having local support and points of contact to maintain, fix, or create accounts for those who have not attended one of these schools.

## 1.0 System Authorization

All new users will be required to complete a DD Form 2875 System Authorization Access Request (SAAR) and register for an ALERTS account.

A Common Access Card (CAC) is required to access the ALERTS application and register for an account.

**Note:** For CID users, DO NOT begin your registration until you have your DD 2875 completed and signed. The completed form must be in PDF format and saved to your local drive.

**Note:** For MP users, the completed form must be in PDF format, saved to your local drive and then emailed to your Installation’s System Administrator for review.

All information contained within ALERTS is restricted by law (5 USC 552a [The Privacy Act]) to those that are authorized to handle criminal justice information. In order to maintain the integrity of this sensitive information it will be accorded proper management and security, and will only be handled by personnel who have been backgrounded for law enforcement work (i.e. LE personnel CID/MP/DACP/Police Admin working for DES/PMO) and who have been trained in the appropriate handling of such sensitive information as required by state and federal law. Activity associated with any aspect of the ALERTS is subject to detailed monitoring and audits of all activity to protect against improper or unauthorized use, access or dissemination of "sensitive information". Unauthorized use, which includes requests, dissemination, sharing, copying, or receipt of ALERTS information, could result in civil proceedings against the offending agency and/or criminal proceedings against any user or other person involved. Violations or misuse may also subject the user and the user's command to administrative sanctions and possible disciplinary action by their command, subject to due process, against its employee(s) and could result in ALERTS access termination.

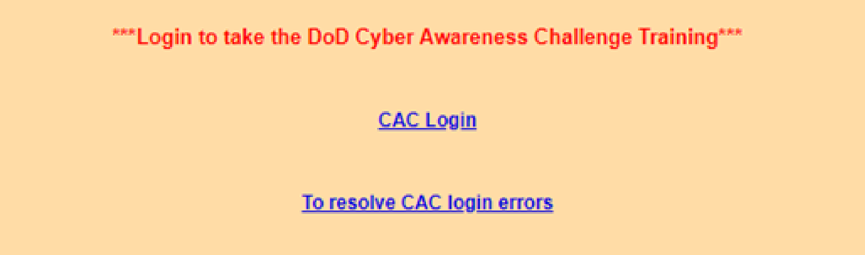
## 1.1 **Annual Information Awareness Training**

All current and requesting users within ALERTS are required to complete and maintain Annual Information Awareness Training, i.e the DoD Cyber Awareness Challenge Training. Students attending training at Fort Leonard Wood that will require computer access must bring with them their current digital or paper copy of their completion certificate. This is mandatory for instructors to verify account access.

> **Note:** The DoD Cyber Awareness Challenge Training must be completed every calendar year. The completion date is required on the initial SAARs (Block 10) requesting ALERTS access.
>
> **Note:** If DoD Cyber Awareness Challenge Training will expire within 60 days of SAAR completion, ALERTS access request, and/or during course attendance, users should obtain a new training certificate to ensure they are current.

Follow the steps below to complete the Cyber Awareness Training course:

1. Launch a compatible web browser (IE9, IE10, Firefox, or Chrome) and navigate to the web address https://cs.signal.army.mil/login.asp.
2. Select **CAC Login.** (Figure 1-1)



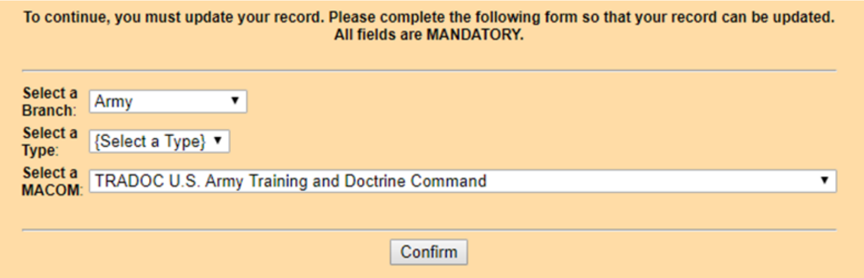
***Login to take the DoD Cyber Awareness Challenge Training***

CAC Login

To resolve CAC login errors

Figure 1-1: Cyber Security Login

3. Select the DOD Email certificate and click **OK.**
4. Select your Branch, Type, and MACOM and click **Confirm.** (Figure 1-2)



To continue, you must update your record. Please complete the following form so that your record can be updated. All fields are MANDATORY.

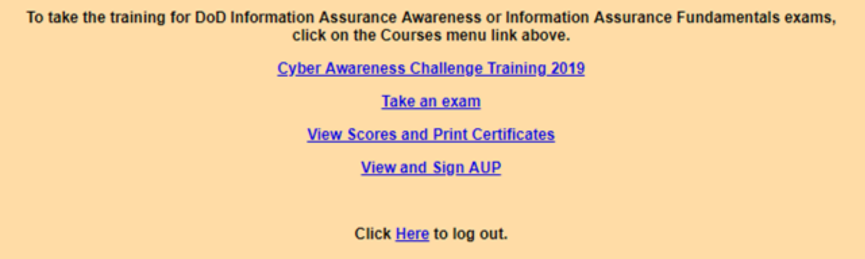
Select a Branch: Army

Select a Type: {Select a Type}

Select a MACOM: TRADOC U.S. Army Training and Doctrine Command

Figure 1-2: Record Update

5. Select **Cyber Awareness Challenge Training** to launch the training page. (Figure 1-3)
6. You can also access the training page by selecting **Take an exam** (Figure 1-3), then click **Go!** on the test selection screen. (Figure 1-4)



To take the training for DoD Information Assurance Awareness or Information Assurance Fundamentals exams, click on the Courses menu link above.

Cyber Awareness Challenge Training 2019

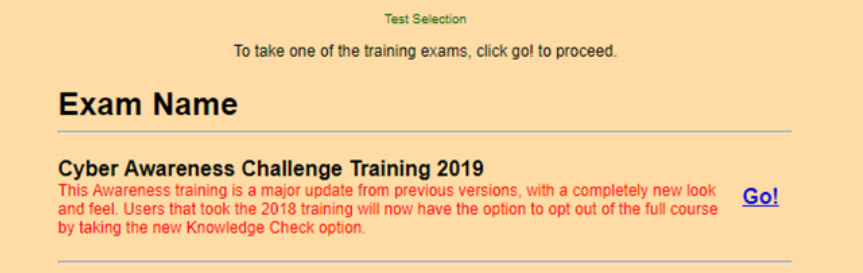
Take an exam

View Scores and Print Certificates

View and Sign AUP

Click Here to log out.

Figure 1-3: Cyber Security Main Menu



Test Selection

To take one of the training exams, click go! to proceed.

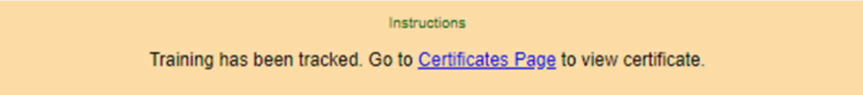
Exam Name

Cyber Awareness Challenge Training 2019

This Awareness training is a major update from previous versions, with a completely new look and feel. Users that took the 2018 training will now have the option to opt out of the full course by taking the new Knowledge Check option.

Figure 1-4: Test Selection

7. Once you have completed the training, select **Certificates Page** on the completion screen (Figure 1-5), or return to the main menu and select **View Scores and Print Certificates.** (Figure 1-3)

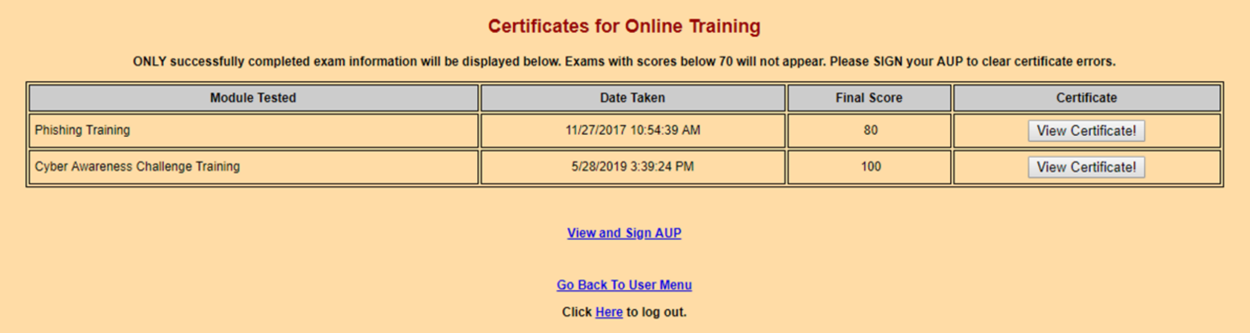


Instructions

Training has been tracked. Go to Certificates Page to view certificate.

Figure 1-5: Training Completion

8. Find your completed Cyber Awareness Challenge Training and click **View Certificates!** (Figure 1-6)



Certificates for Online Training

ONLY successfully completed exam information will be displayed below. Exams with scores below 70 will not appear. Please SIGN your AUP to clear certificate errors.

| Module Tested | Date Taken | Final Score | Certificate |
|---|---|---|---|
| Phishing Training | 11/27/2017 10:54:39 AM | 80 | View Certificate! |
| Cyber Awareness Challenge Training | 5/28/2019 3:39:24 PM | 100 | View Certificate! |

View and Sign AUP

Go Back To User Menu

Click Here to log out.

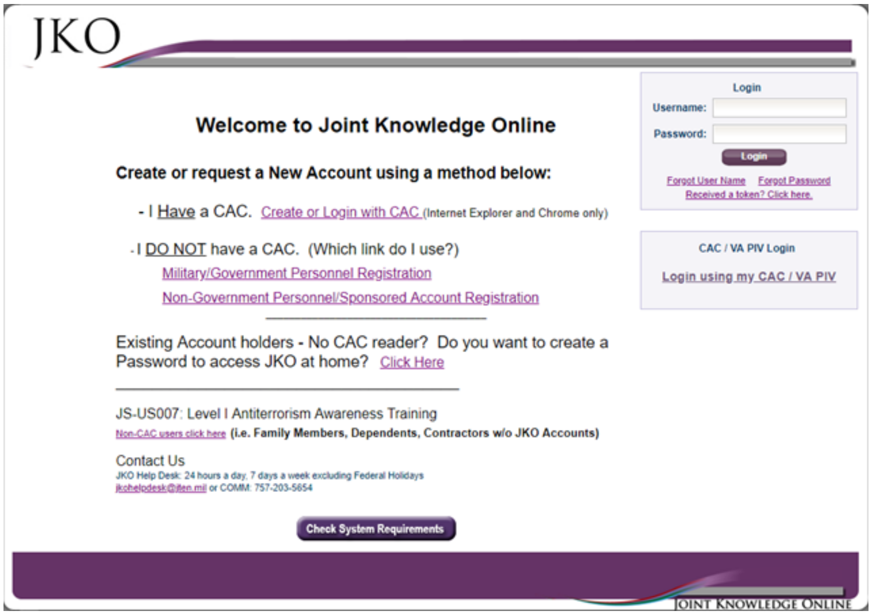
Figure 1-6: Scores and Certificates

### 1.1.1 **Joint Knowledge Online (JKO) Alternate Training Site**

The Annual Information Awareness Training can also be conducted via JKO if students are unable to access the site link in Section 1.2.

Follow the steps below to complete the Cyber Awareness Training course through JKO:

1. Launch a compatible web browser (IE9, IE10, Firefox, or Chrome) and navigate to the web address https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf.
2. Select **Login using my CAC / VA PIV.** (Figure 1-7)



Welcome to Joint Knowledge Online

Create or request a New Account using a method below:

- I Have a CAC. Create or Login with CAC (Internet Explorer and Chrome only)

- I DO NOT have a CAC. (Which link do I use?)
Military/Government Personnel Registration
Non-Government Personnel/Sponsored Account Registration

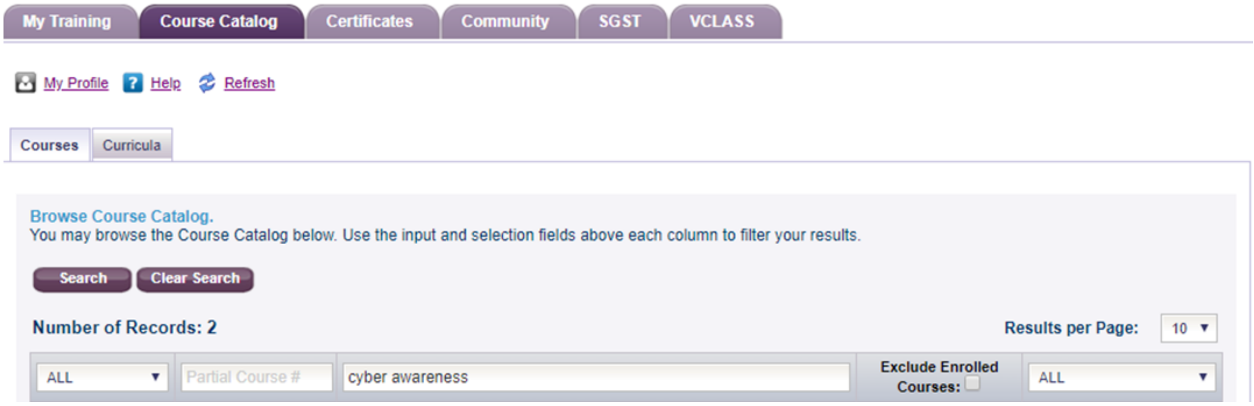
Existing Account holders - No CAC reader? Do you want to create a Password to access JKO at home? Click Here

JS-US007: Level I Antiterrorism Awareness Training
Non-CAC users click here (i.e. Family Members, Dependents, Contractors w/o JKO Accounts)

Contact Us
JKO Help Desk: 24 hours a day, 7 days a week excluding Federal Holidays
jkohelpdesk@jten.mil or COMM: 757-203-5654

Figure 1-7: JKO Login

3. Select the DOD Email certificate and click **OK.**
4. Select the Course Catalog tab, search for "Cyber Awareness" in the Title Key Word, and click on **Search.** (Figure 1-8)



Browse Course Catalog.
You may browse the Course Catalog below. Use the input and selection fields above each column to filter your results.

Number of Records: 2

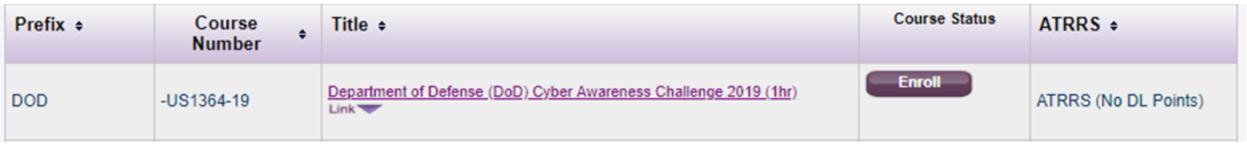
Results per Page: 10

cyber awareness

Exclude Enrolled Courses: □

Figure 1-8: Course Catalog Search

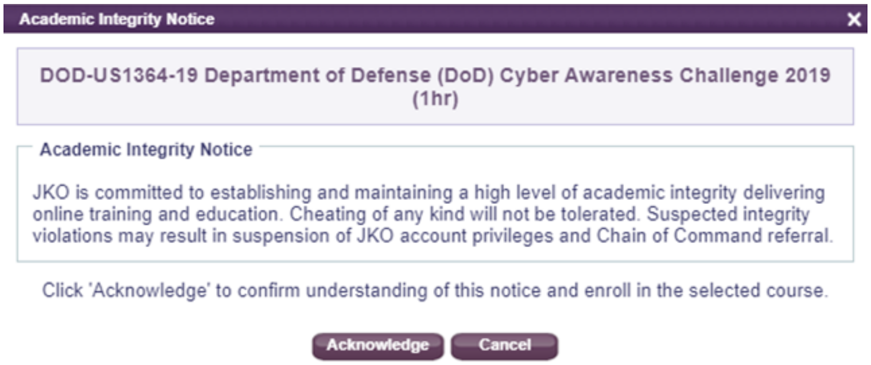
5. Find Course Number "DOD-US1364-19" and click **Enroll.** (Figure 1-9)



| Prefix ⬍ | Course Number ⬍ | Title ⬍ | Course Status | ATRRS ⬍ |
|---|---|---|---|---|
| DOD | -US1364-19 | Department of Defense (DoD) Cyber Awareness Challenge 2019 (1hr)<br>Link | Enroll | ATRRS (No DL Points) |

Figure 1-9: Course Selection

6. Read the Academic Integrity Notice and click **Acknowledge.** (Figure 1-10)



Academic Integrity Notice ✕

DOD-US1364-19 Department of Defense (DoD) Cyber Awareness Challenge 2019 (1hr)

Academic Integrity Notice

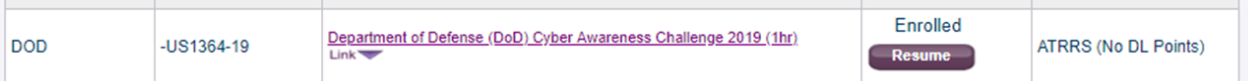
JKO is committed to establishing and maintaining a high level of academic integrity delivering online training and education. Cheating of any kind will not be tolerated. Suspected integrity violations may result in suspension of JKO account privileges and Chain of Command referral.

Click 'Acknowledge' to confirm understanding of this notice and enroll in the selected course.

Acknowledge Cancel

Figure 1-10: Academic Integrity Notice

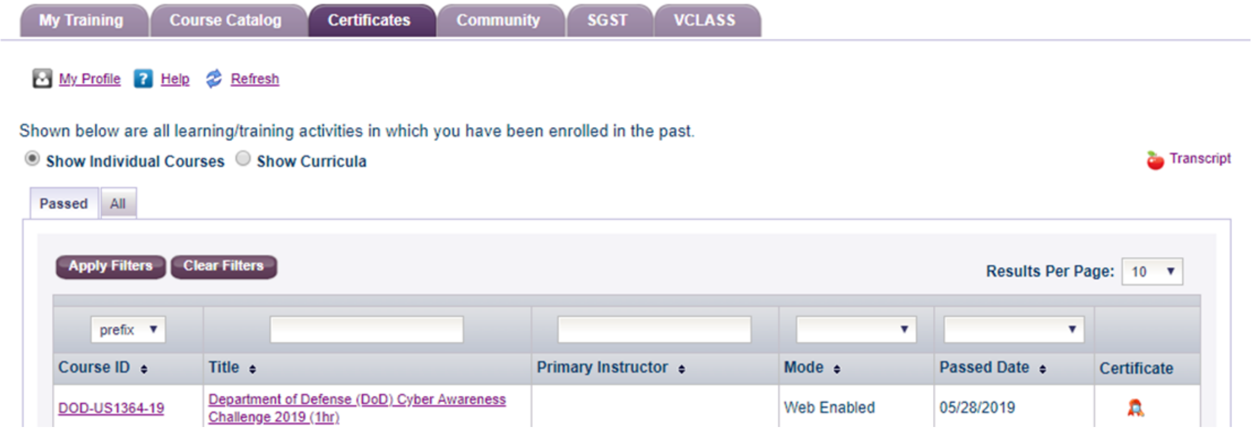
7. Click **Resume** to launch the training course. (Figure 1-11)



| | | | | |
|---|---|---|---|---|
| DOD | -US1364-19 | Department of Defense (DoD) Cyber Awareness Challenge 2019 (1hr)<br>Link | Enrolled<br>Resume | ATRRS (No DL Points) |

Figure 1-11: Resume Training

8. Once training is complete, select the Certificates tab. Find your completed Cyber Awareness Challenge and click 🎖 . (Figure 1-12)



Shown below are all learning/training activities in which you have been enrolled in the past.

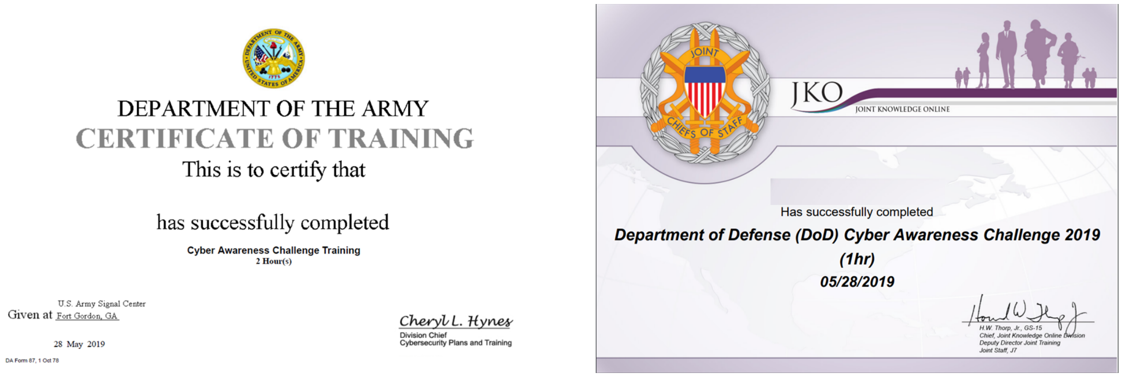
● Show Individual Courses ○ Show Curricula

Results Per Page: 10

| Course ID ⬍ | Title ⬍ | Primary Instructor ⬍ | Mode ⬍ | Passed Date ⬍ | Certificate |
|---|---|---|---|---|---|
| DOD-US1364-19 | Department of Defense (DoD) Cyber Awareness Challenge 2019 (1hr) | | Web Enabled | 05/28/2019 | 🎖 |

Figure 1-12: Resume Training

9. Below are the two authorized training certificates that will be accepted. (Figure 1-13)



DEPARTMENT OF THE ARMY
CERTIFICATE OF TRAINING
This is to certify that

has successfully completed

**Cyber Awareness Challenge Training**
**2 Hour(s)**

Given at U.S. Army Signal Center
Fort Gordon, GA

28 May 2019

Cheryl L. Hynes
Division Chief
Cybersecurity Plans and Training

DA Form 87, 1 Oct 78

JKO
JOINT KNOWLEDGE ONLINE

Has successfully completed
***Department of Defense (DoD) Cyber Awareness Challenge 2019***
***(1hr)***
***05/28/2019***

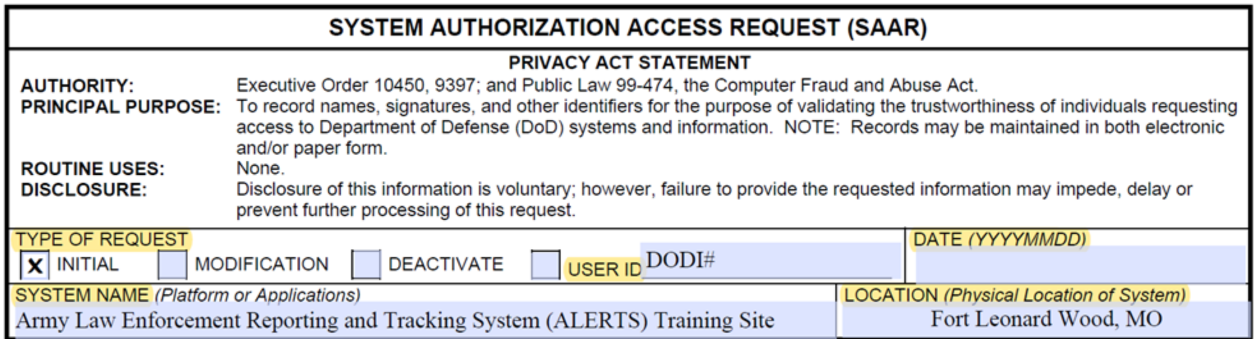
*H.W. Thorp, Jr., GS-15*
*Chief, Joint Knowledge Online Division*
*Deputy Director Joint Training*
*Joint Staff, J7*

Figure 1-13: Annual Information Awareness Training Authorized Certificates

## 1.2 **ALERTS Training Account, DD Form 2875 (SAAR)**

Follow the steps below to complete a DD Form 2875, System Authorization Access Request (SAAR), for a new or existing ALERTS training account:

1. Open a new DD Form 2875.
2. In TYPE OF REQUEST block, check 'INITIAL' and write "DODI#" followed by your DODI in the 'USER ID' section. (Example: DODI#1234567890)
3. Complete DATE block.
4. In SYSTEM NAME block, write "Army Law Enforcement Reporting and Tracking System (ALERTS) Training Site".
5. In LOCATION block, write your installation for which you are requesting access to ALERTS. (Example: "Fort Leonard Wood, MO") (Figure 1-14)



**SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)**

**PRIVACY ACT STATEMENT**

**AUTHORITY:** Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.
**PRINCIPAL PURPOSE:** To record names, signatures, and other identifiers 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.

TYPE OF REQUEST
☒ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID DODI#

DATE *(YYYYMMDD)*

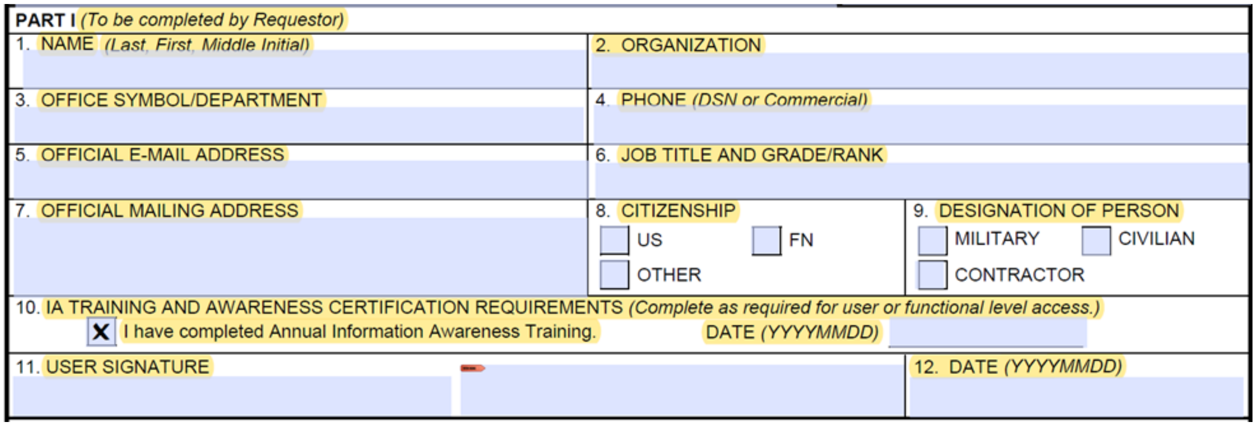
SYSTEM NAME *(Platform or Applications)*
Army Law Enforcement Reporting and Tracking System (ALERTS) Training Site

LOCATION *(Physical Location of System)*
Fort Leonard Wood, MO

Figure 1-14: SAAR Header

6. Complete PART I (Blocks 1-12). (Figure 1-15)

**Note:** Ensure that you write your signature name in Block 11, enter the current date in Block 12, and then digitally sign the document. Once you digitally sign the SAAR, all blocks in PART I will be locked.



PART I *(To be completed by Requestor)*

| | | |
|---|---|---|
| 1. NAME *(Last, First, Middle Initial)* | 2. ORGANIZATION | |
| 3. OFFICE SYMBOL/DEPARTMENT | 4. PHONE *(DSN or Commercial)* | |
| 5. OFFICIAL E-MAIL ADDRESS | 6. JOB TITLE AND GRADE/RANK | |
| 7. OFFICIAL MAILING ADDRESS | 8. CITIZENSHIP<br>□ US □ FN<br>□ OTHER | 9. DESIGNATION OF PERSON<br>□ MILITARY □ CIVILIAN<br>□ CONTRACTOR |

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*

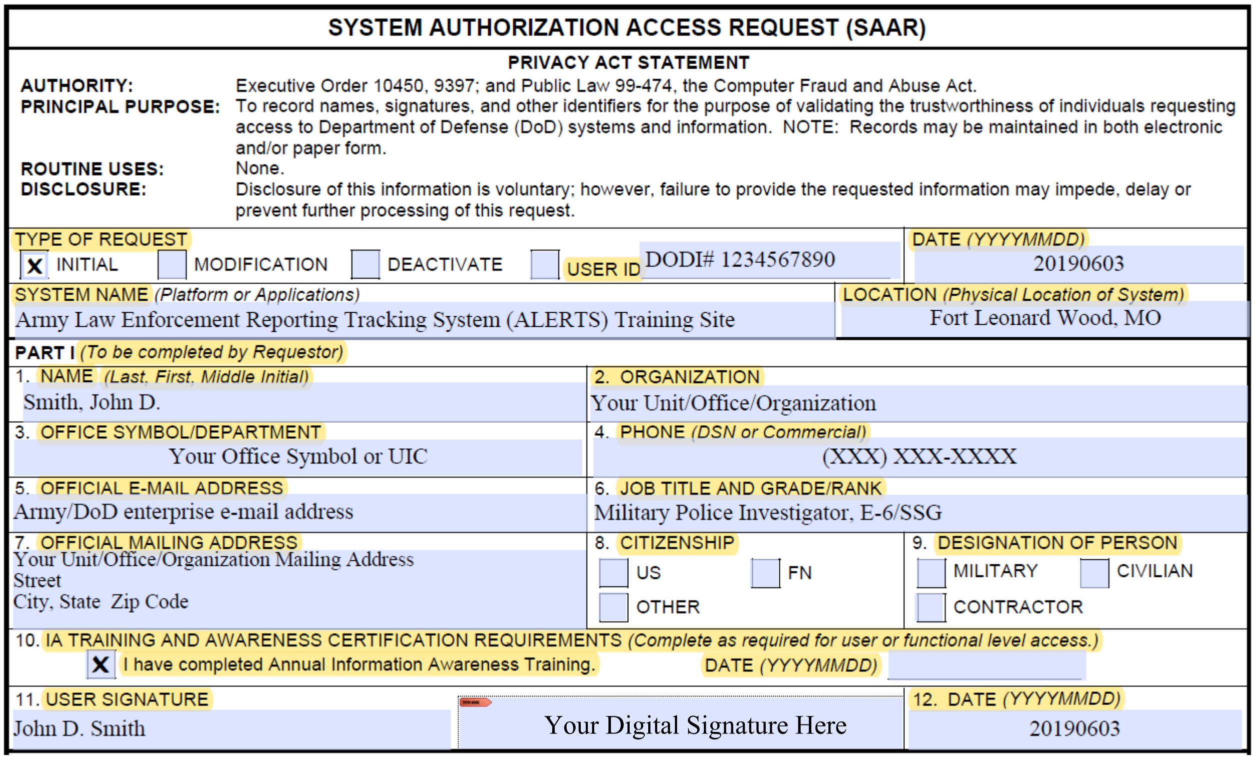
☒ I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)*

11. USER SIGNATURE

12. DATE *(YYYYMMDD)*

Figure 1-14: SAAR PART I

**Note:** Users who have an existing ALERTS training account and are completing the SAAR for the first time or are updating an existing SAAR on file, must submit the completed form to their local or installation System Administrator for them to upload the document into ALERTS.



**SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)**

**PRIVACY ACT STATEMENT**

**AUTHORITY:** Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

**PRINCIPAL PURPOSE:** To record names, signatures, and other identifiers 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.

TYPE OF REQUEST: ☒ INITIAL □ MODIFICATION □ DEACTIVATE □ USER ID DODI# 1234567890

DATE *(YYYYMMDD)*: 20190603

SYSTEM NAME *(Platform or Applications)*: Army Law Enforcement Reporting Tracking System (ALERTS) Training Site

LOCATION *(Physical Location of System)*: Fort Leonard Wood, MO

PART I *(To be completed by Requestor)*

| | | |
|---|---|---|
| 1. NAME *(Last, First, Middle Initial)*<br>Smith, John D. | 2. ORGANIZATION<br>Your Unit/Office/Organization | |
| 3. OFFICE SYMBOL/DEPARTMENT<br>Your Office Symbol or UIC | 4. PHONE *(DSN or Commercial)*<br>(XXX) XXX-XXXX | |
| 5. OFFICIAL E-MAIL ADDRESS<br>Army/DoD enterprise e-mail address | 6. JOB TITLE AND GRADE/RANK<br>Military Police Investigator, E-6/SSG | |
| 7. OFFICIAL MAILING ADDRESS<br>Your Unit/Office/Organization Mailing Address<br>Street<br>City, State Zip Code | 8. CITIZENSHIP<br>□ US □ FN<br>□ OTHER | 9. DESIGNATION OF PERSON<br>□ MILITARY □ CIVILIAN<br>□ CONTRACTOR |

10. IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*

☒ I have completed Annual Information Awareness Training. DATE *(YYYYMMDD)*

11. USER SIGNATURE: John D. Smith — Your Digital Signature Here

12. DATE *(YYYYMMDD)*: 20190603

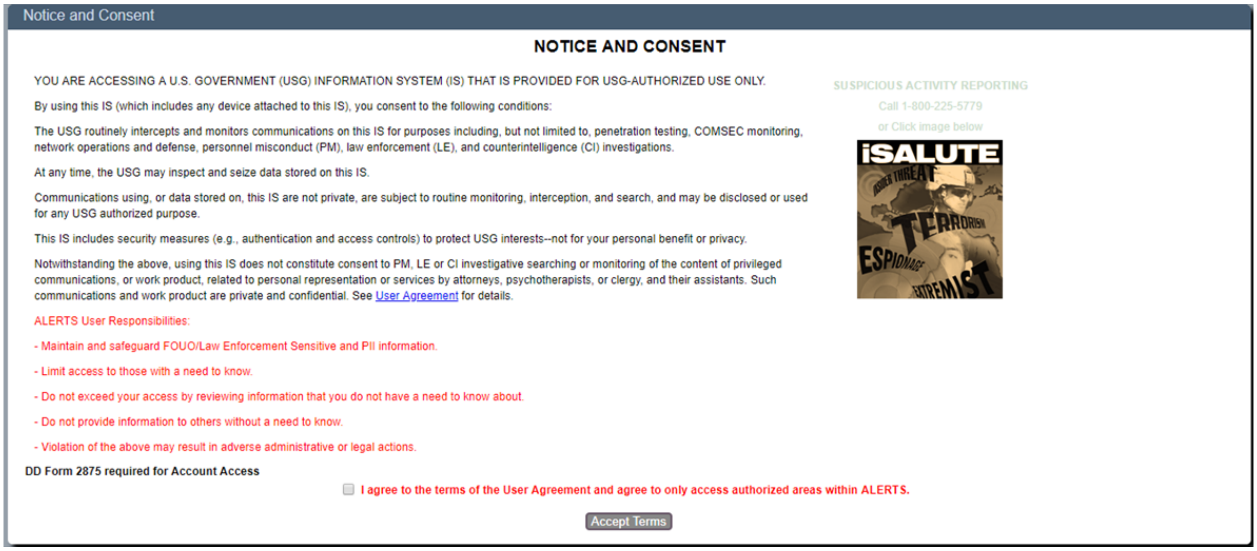
Figure 1-15: Completed SAAR (ALERTS training account)

# 2.0 **Registering for an ALERTS Training Account**

Follow the steps below to register for an ALERTS training account:

> **Note:** Users must have completed their Annual Information Awareness Training and a completed SAAR in digital format before requesting for an ALERTS training account.

1. Launch a compatible web browser (IE9, IE10, Firefox, or Chrome) and navigate to the web address https://www.cimstrain.army.mil.
2. Select the Authentication (PIV) certificate and click **OK.**
3. When prompted, enter your PIN and click **OK.**
4. You will then see the Notice and Consent. (Figure 2-1)



Notice and Consent

NOTICE AND CONSENT

YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS PROVIDED FOR USG-AUTHORIZED USE ONLY.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

At any time, the USG may inspect and seize data stored on this IS.

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

ALERTS User Responsibilities:

- Maintain and safeguard FOUO/Law Enforcement Sensitive and PII information.

- Limit access to those with a need to know.

- Do not exceed your access by reviewing information that you do not have a need to know about.

- Do not provide information to others without a need to know.

- Violation of the above may result in adverse administrative or legal actions.

DD Form 2875 required for Account Access

SUSPICIOUS ACTIVITY REPORTING

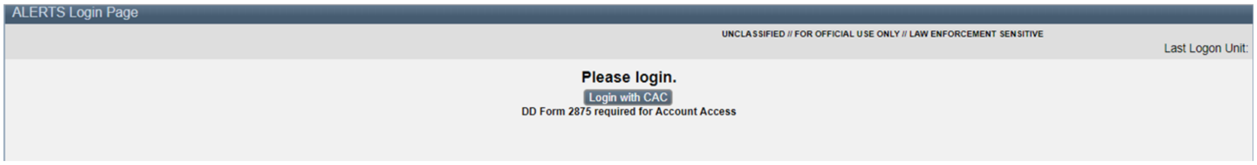
Call 1-800-225-5779

or Click image below

□ I agree to the terms of the User Agreement and agree to only access authorized areas within ALERTS.

Figure 2-1: ALERTS Notice and Consent

5. Read the Notice and Consent, check the "I agree…"  checkbox, and then click **Accept Terms** to accept the Notice and Consent User Agreement.
6. You will then see the Login page. (Figure 2-2)



ALERTS Login Page

UNCLASSIFIED // FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE

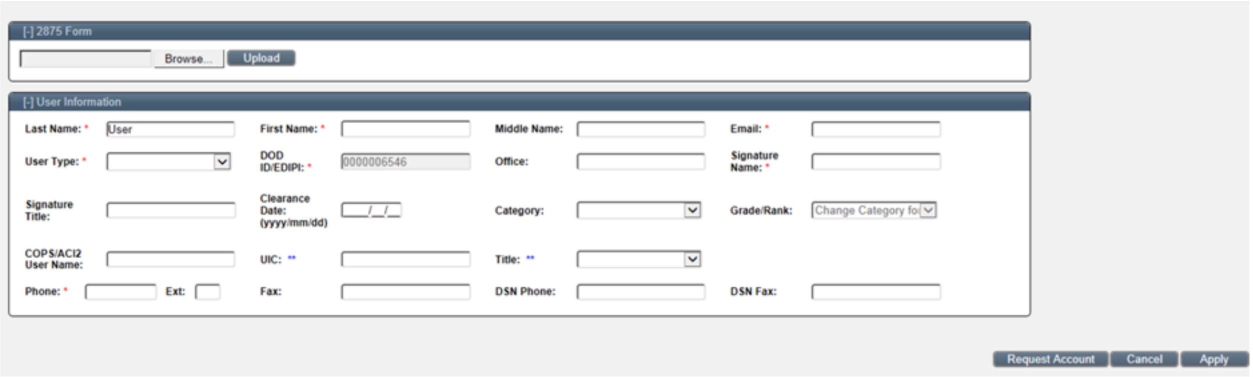
Last Logon Unit:

Please login.

DD Form 2875 required for Account Access

Figure 2-2: ALERTS Login Page

7. Click **Login with CAC.**
8. Next, you will see the ALERTS Registration page. (Figure 2-3)



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Last Name: * | User | First Name: * | | Middle Name: | | Email: * | |
| User Type: * | | DOD ID/EDIPI: * | 0000006546 | Office: | | Signature Name: * | |
| Signature Title: | | Clearance Date: (yyyy/mm/dd) | __/__/__ | Category: | | Grade/Rank: | Change Category fo |
| COPS/ACI2 User Name: | | UIC: ** | | Title: ** | | | |
| Phone: * | Ext: | Fax: | | DSN Phone: | | DSN Fax: | |

Figure 2-3: ALERTS Registration Page

9. Click **Browse...** and select your completed DD Form 2875. Then, click **Upload.**
10. Complete the Required (*) and Mandatory (**) fields, at a minimum. Additional information for each field is provided in the table below.

| Field | Description |
|---|---|
| Last Name | The Last Name will be populated with the user's Last Name from their Common Access Card (CAC). |
| | This field can be modified, if needed. |
| First Name | The First Name will be populated with the user's First Name from their Common Access Card (CAC). |
| | This field can be modified, if needed. |
| Middle Name | The Middle Name will be populated with the user's Middle Name from their CAC. |
| | This field can be modified, if needed. |
| Email | The Email will be populated with the email associated with the user's Common Access Card (CAC). |
| | This field can be modified, if needed. |
| | The user must enter their Enterprise Email address in the field. |
| | Example: john.doe.civ@mail.mil |
| User Type | The values include CID, CRC, and Police (i.e. MPs, MPI, & DACP). |
| DOD ID/EDIPI | The DOD ID/EDIPI is associated with the user's Common Access Card (CAC). |
| Office | A text field for the user's Office information. |
| | Example: DES, CID G6 |
| Signature Name | The value entered in this field will display in the Report Prepared By and/or the Report Approved By section of the Investigative Reports. |
| | It is recommended the user enter their First Name, Middle Initial, and Last Name |
| | Example: John B. Doe |
| Signature Title | The value entered in this field will display in the Report Prepared By and/or the Report Approved By section of the Investigative Reports. |
| | Example: SGT, SSG, 1LT, SA, SAC, TC |

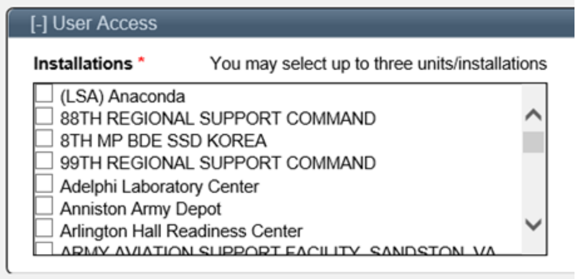
Table 1: User Registration Field Information

| Field | Description |
|---|---|
| Clearance Date | The user's Clearance date. The date format is YYYY/MM/DD. |
| | This is only required when approving a CID account. |
| Category | A drop-down list including Army, Air Forces, Civilian, Marines, etc. |
| Grade/Rank | The values are linked to the Category drop-down field. Values will display in the drop-down field when a Category is selected. |
| COPS/ACI2 User Name | The user's user name from the legacy applications. This information will assist with migrating open cases from ACI2 and COPS. |
| UIC | The user's Unit Identification Code (UIC). The UIC is a six digit alphanumeric value. |
| | Example: W12345 |
| Title | A drop-down list of values including SA, DET, INV, Mr., Mrs., etc. |
| Phone | The user's commercial telephone number. |
| Ext | The extension for the user's commercial telephone number. |
| Fax | The user's fax number. |
| DSN Phone | The user's DSN telephone number. |
| DSN Fax | The user's DSN fax number. |

Table 1 (cont.): User Registration Field Information

11. Once the User Type is selected, the User Access section will appear below the User Information section. Select the appropriate unit or installation. You may select up to three units or installations. At a minimum, Fort Leonard Wood and your local unit/installation should be chosen. (Figure 2-4 & Figure 2-5)

**Note:** If the User Type is Police, you will see the Installations selection. If the User Type is CID, you will see the Units selection.

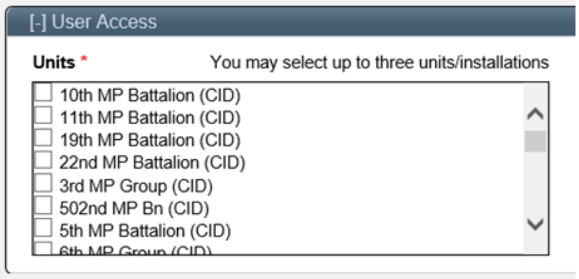


[-] User Access

Installations * You may select up to three units/installations

□ (LSA) Anaconda
□ 88TH REGIONAL SUPPORT COMMAND
□ 8TH MP BDE SSD KOREA
□ 99TH REGIONAL SUPPORT COMMAND
□ Adelphi Laboratory Center
□ Anniston Army Depot
□ Arlington Hall Readiness Center
□ ARMY AVIATION SUPPORT FACILITY, SANDSTON, VA

Figure 2-4: User Type (Police)



[-] User Access

Units * You may select up to three units/installations

□ 10th MP Battalion (CID)
□ 11th MP Battalion (CID)
□ 19th MP Battalion (CID)
□ 22nd MP Battalion (CID)
□ 3rd MP Group (CID)
□ 502nd MP Bn (CID)
□ 5th MP Battalion (CID)
□ 6th MP Group (CID)

Figure 2-5: User Type (CID)

12. Once complete, click **Apply** to save your information and then click **Request Account** to complete the registration. (Figure 2-6)

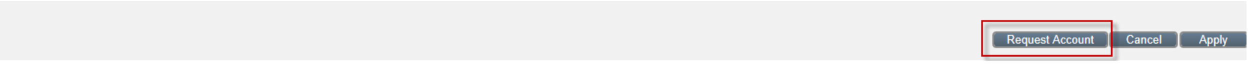
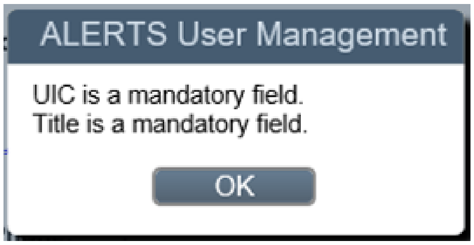


Figure 2-6: Request Account Button

**Note:** Required (*) and Mandatory (**) fields are both necessary to request for an account. If any necessary fields are missing when you click **Request Account**, a pop-up will appear. (Figure 2-7)

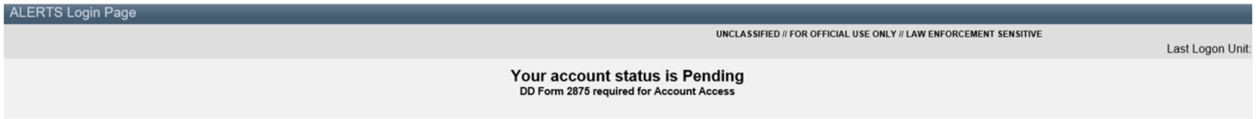


ALERTS User Management

UIC is a mandatory field.
Title is a mandatory field.

Figure 2-7: Missing Required or Mandatory Fields

**Note:** System Administrators and SACs will receive an email notification when any user registers for an account within their installation or unit. An email confirmation will be sent to the user once the account has been approved. Until a user account is approved, the user will see the Account Pending screen whenever they attempt to login to ALERTS. (Figure 2-8)



ALERTS Login Page

UNCLASSIFIED // FOR OFFICIAL USE ONLY // LAW ENFORCEMENT SENSITIVE

Last Logon Unit:

Your account status is Pending
DD Form 2875 required for Account Access

Figure 2-8: ALERTS Account Pending

## 2.1 Users with existing ALERTS Training Accounts

All users that have an existing ALERTS training account need to ensure that their account is up-to-date and active before attending training.

1. If your account is active, ...

   a. Check with your ALERTS Training Site System Administrator for your installation/unit to verify that you have an updated SAAR uploaded. (See Section 1.2 for assistance.)
   b. Print out and bring your most recent DoD Cyber Awareness Training certificate to your training/course. (See Section 1.1 for assistance.)

2. If your account is Expired or has been PCSed, ...

   a. Contact your ALERTS Training Site System Administrator for your installation/unit to have your account revalidated or brought into your current installation/unit, as well as adding Fort Leonard Wood to your authorized installations.

b. Update/complete a SAAR for your account. (See Section 1.2)
c. Print out and bring your most recent DoD Cyber Awareness Training certificate to your training/course. (See Section 1.1 for assistance.)

## 3.0 **Account Issues/Questions**

If there are any questions or issues with an ALERTS training account,...

1. Contact your installation/unit ALERTS System Administrator for assistance and guidance.
2. If futher assistance is required, contact the CIMS Help Desk at usarmy.belvoir.usacidc.list.cims-help-desk@mail.mil.
3. If you are still having issues resolving your ALERTS training account and/or have already started a course at either USAMPS or USACPA, contact your Course Manager or Course POC for assistnace.
4. USAMPS ALERTS training instructors are available for assistance anytime at usarmy.leonardwood.mp-schl.mbx.alerts@mail.mil; however, please attempt to work through appropriate channels first.