



Army Training and Certification Tracking System – User’s Guide

As of 8 February 2016



This User’s Guide serves as a source for details of the main areas of functionality the users of the ATC system need to know as they create, navigate, update and maintain their ATCTS accounts/profiles.

Table of Contents

ATCTS (Army Training and Certification Tracking System) Information.....	2
WEBPAGE NAVIGATION FOR ATCTS MAIN PAGE (homepage) https://atc.us.army.mil/iastar/index.php	3
• Disclaimer (on every page).....	3
• Left Side Navigation Links.....	4
<u>Top Right Side Helpful Links:</u>	
• Register - How To Register.....	5
• Login - How To Login (To Old or New Accounts).....	10
• Users with more than one ATCTS account).....	13
• Help - Contact Information.....	14
<u>How to get around and populate your ATCTS account:</u>	
• Your ATCTS IA Training Profile(How to).....	15
• Online Training Links.....	18

ATCTS (Army Training and Certification Tracking System) Information:

- This user guide is to help individuals navigate the Army Training and Certification Tracking System (ATCTS).
 - The system enables users to track their training from various Department of Defense and Army Systems.
 - ATCTS has an automatic feed from the following sites - which imports directly into the individual's profiles every 24 to 48 hours after course completion.
 - Skillport Army e-Learning Program
 - Army Virtual Training Center
 - Fort Gordon Signal Site
 - ATCTS has an automatic feed from the following sites - which imports directly into the individual's profiles on the 1st and 15th of each month after course completion and release from the CompTia training site.
 - DoD Manpower Data Center (DMDC)
 - ATCTS has an indirect feed from:
 - Department of Homeland Security Federal Virtual Training Environment
 - The Data Feeds capture the name of the training, date of completion and the website the training was completed on. Users must go back to the website that the training was completed on to view and print the certificate of completion/training.
 - ATCTS support in regards to Login, Registration, Unit Assignment and Training/Certification issues can be emailed to the IASTAR online support at support@iastar.net 816-842-6260 from 0800-1600 CST Monday-Friday or the Army CIO/G6 Training and Certification Branch at usarmy.belvoir.hqda-cio-g-6.mbx.training-and-certification@mail.mil
-

WEBPAGE NAVIGATION FOR ATCTS MAIN PAGE (Home Page):<https://atc.us.army.mil/iastar/index.php>

Disclaimer - The disclaimer link appears at the bottom of each page of the ATC Website

Disclaimer

References or links to commercial and other non-official sites are for information purposes only and are provided for the convenience of the users of this system. Such references are not endorsements by the Department of Defense (DoD), Department of the Army (DA), Fort Gordon, or the School of Information Technology (SIT). Viewpoints expressed, if any, are those of the site's contributors and do not represent official or unofficial views of DoD, DA, Ft. Gordon, or the SIT.

Copyright Warning:

Many images in this site are copyrighted material. The author has obtained permission to use these images and sounds for the development of this site. Permission to use these images and sounds DO NOT extend to the users of this site. Use of these images and sounds can constitute a copyright infringement and is prohibited by law. This site is intended to support all individuals performing any of the IA FUNCTIONS described in DoD 8140.1M and the IA Training BBP (Best Business Practices).

Privacy and Security Notice

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.

Powered By  © 2005-15 WillCo Technologies, Inc. All Rights Reserved. **Disclaimer**

Left Side Navigation Links

Home Page: Left Side Menu



The Home link will bring you back to the Home page from any other page in the system.

If you are **not logged in**, the Home page Left Side Navigation Menu displays Registration/Login links. If you **are logged** into the system, the Home page will display a Profile/Account Info link on the Left Side Navigation Menu

Concise information contained in each link will assist you in your navigation of the ATCTS website

The Home link brings you back to the Home page from any page on the site

The News link provides current and archived information, resources and alerts

The DOD CAC Training link provides information and links for this training – which is an annual requirement at <https://ia.signal.army.mil/DoDIAA/default.asp>.

The heading for the next 3 links regarding User Profiles, Accounts and Navigation

The Profile link takes you to your account “My Profile” page where you review Training/Certificates along with you IA Position entries/assessments for required training

This Account page allows updates of personal information; inclusive of you Enterprise email address, phone, rank, and unit assignment (per manager approval)

This link provides the system User’s/ Manager’s Guide and Frequently Asked Questions (FAQ) and Training Videos

Link displaying the full statement regarding IA Training & Certification Mission – Awareness, Education and Training

Website Assistance Information and Signal Command/**FCIO Contact Information**

Links to online classes /exams/ certifications for training to meet compliancy standards

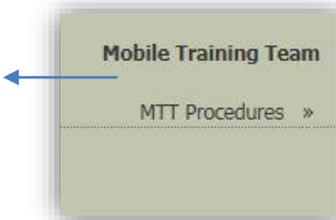
IA positions, General and Power Users according to personnel responsibilities.

Compliance & Regulation Information documents, Voucher and Assessment documents, Information Templates and other documents

Self-assessment tools to help prepare for the CISA and CISM exams; Access to a rich library of cyber security and Information Assurance training; Voucher requests; CompTIA Pre-assessment Procedures; GIAC short assessment for SANS training

The Mobile Training Team Links are displayed, once the user has logged in to the ATCTS site

Manager and User Procedures for Mobile Training Team (MTT) Courses [Baseline Certification Training and Computing Environment Training for Army organizations]



ATCTS Managers would have an additional link:

← (MTT Administrators)

Top Right Side Helpful Links Home Page: Right Side Menu

Located at the top, right corner of the home page

Registration /Login/Help Links

1. **register** links to:
<https://atc.us.army.mil/iastar/register.php>
2. **login** links to: <https://atc.us.army.mil/iastar/login.php>
3. **help:** links to User’s and Manager’s Guides and the Contact Information for user resources.



“How to Register”

1. Type or copy and paste this **URL** in your IE (Internet Explorer) web browser:
<https://atc.us.army.mil/index.php>
2. Click the Registration link at the top right of the Front Page or ...
3. Click the “Registration Information” link on the left side of the page
4. Complete the Registration Form:

A screenshot of a web form titled "User Registration Form". The form contains several input fields and dropdown menus. At the top, it says "An AKO or Enterprise Email Address is Required to Register. All Remaining Fields are Required." The fields include: First Name, Middle Initial, Last Name, Suffix (dropdown), AKO Email Address, Enterprise Email Address, Phone Number, Personnel Type (dropdown), Personnel Security Standard (dropdown with a link to "see descriptions"), Degree Type (dropdown, currently set to "Associate Degree"), Occupational Specialty (dropdown, currently set to "None" with "Step 2" below it), and a checkbox "I have the specialty type INFOSEC on my SF50". Below these is a section "Select Unit Placement (4 steps or use search)" with fields for "HQ Alignment (MACOM)", "HQ Alignment Subordinate Unit", "Signal Command/Function Chief Info Ofc (SC/FCIO)", and "SC/FCIO Subordinate Unit". A "Register" button is at the bottom.

“How to Register” continued

5. **Be sure to use your ENTERPRISE e-mail address, example: john.doe.civ@mail.mil.**
 - **AKO has shut down AKO email addresses.**
 - **When registering with AKO email address please contact the Army CIO/G6 or STAR Support helpdesk for an access code. The system will be moving to Single Sign on in FY16.**
 - **Also consider one of these helpful links:**

Assistance for users that are yet having issues with the migration from AKO to Enterprise

1. <http://akoarmymil.com/accessing-enterprise-email-owa/>
2. <http://akoarmymil.com/ako-webmail-migration/>

This is a video that is helpful as well.

3. <https://www.youtube.com/watch?v=UTebDmgjgNY>

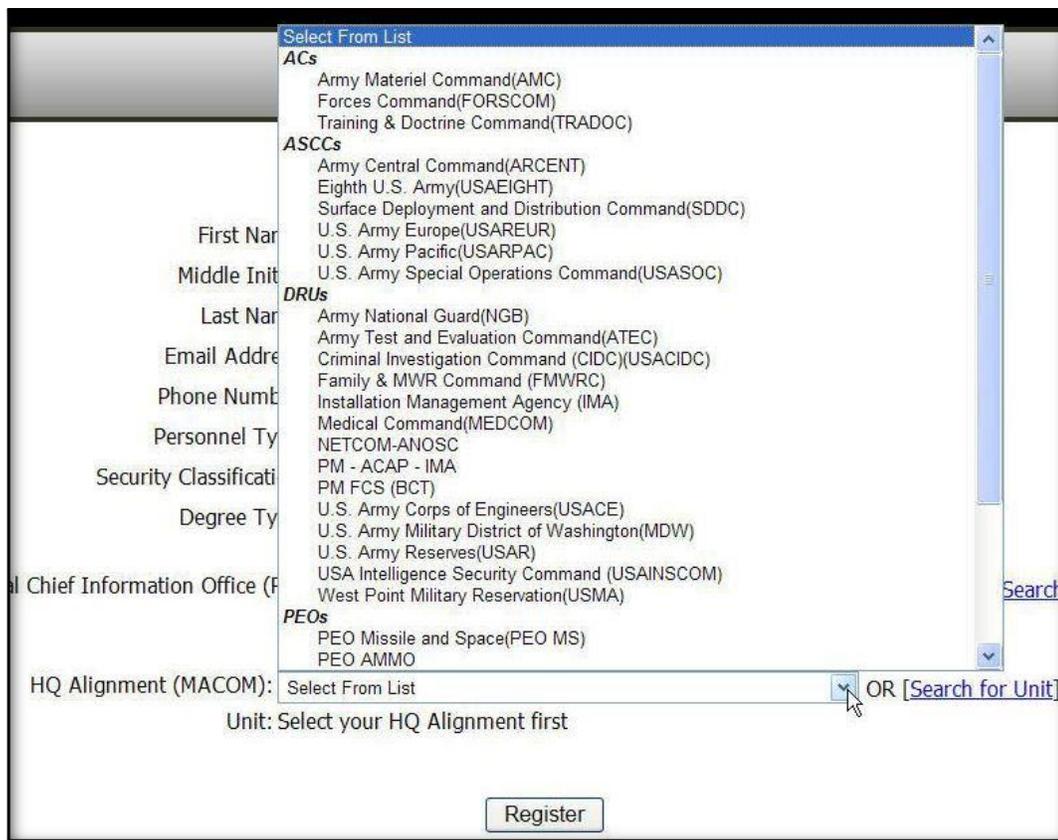
AKO alternates	Enterprise alternates
<p>In addition to @us.army.mil, the following alternate domains are acceptable entries for the AKO Email Address field.</p> <ol style="list-style-type: none"> 1. @us.af.mil 2. @navy.mil 3. @usmc.mil 4. @soc.mil 5. @usace.army.mil <p>If you use one of these alternate domains, please select "Other Service Branch" as your Personnel Type below.</p>	<p>The standard naming schema is {first name}{.}{middle initial}{.}{last name}{sequence number}{.} {persona type code}@mail.mil. Example: John.E.Smith26.civ@mail.mil Valid persona type codes are listed below:</p> <ol style="list-style-type: none"> 1. .mil 2. .civ 3. .ctr 4. .naf 5. .nfg 6. .fm 7. .ln 8. .vol

6. Unit Selection:

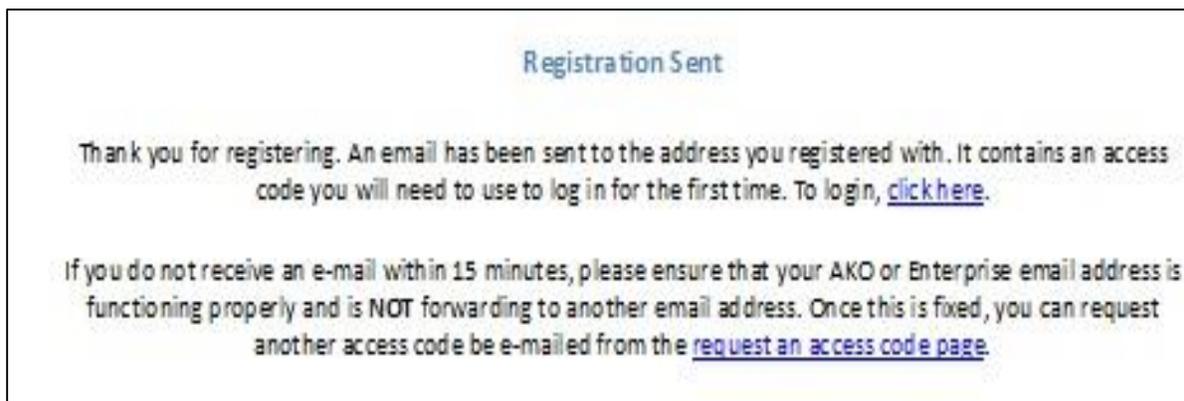
- a. The **Signal Command** is where you are
- b. The **HQ Alignment** is the higher element the command of who you report to.
- c. Select your **HQ Alignment/Major Command** via the SELECT FROM LIST (dropdown box) - The structure reflects the new Army alignment (AC=Army Commands, ASCC = Army Service Command Components, DRU = Direct Reporting Unit, and PEO = Program Executive Office)
- d. Click to select your **subordinate unit or Search for Unit** if you know the name of your organization. Once the organization is found, click on select. If an SC/FCIO pops up for selections then select YES.

7. Unit Selection: continued:

- a. Select your **Signal/FCIO Unit command** – The physical location of your organization (generally the same as the HQ Alignment) via the SELECT FROM LIST (dropdown box)



- 8. Upon completion of the registration information, click on the **Register Button**. The following message will be displayed;



- 9. Go back to <https://atc.us.army.mil/login/php>, log on using the ACCESS CODE sent to your registered EMAIL ADDRESS (be sure to COPY and PASTE, don't try to type it). Complete the questionnaire – which pops up upon a successful login.

10. The **QUESTIONNAIRE** helps the ATCTS determine your DOD IA Workforce authorization and access for your Cybersecurity roles and responsibilities in compliance with the Army Training & Certification Best Business Practices (BBP). When you complete the questionnaire, your profile assignment will appear with a link to the My Profile page – where you can view all your IA training.

Access **QUESTIONNAIRE**

1) * Choose the answer that best describes your access to the Information System (IS) for your Primary Duty Position

- Manager**
A user with management or data owner access to the IS. These users would include (but are not limited to) these functional responsibility positions: IA Director, IA Deputy Director, SC/FCIO, IAPM and IAM.
- Technical User**
A user with system administrators (SA), IANM, or network administrator (NA) responsibilities who performs (but is not limited to) such duties as (a)Enforce the IS security guidance policies, (b)Enforce system access, operation, maintenance, or disposition requirements or (c) Review and verify currency of user accounts.
- Computer Network Defense - Service Provider**
A user that works with/in the Network Operations Centers (NOC), Network Operations Security Centers (NOSC), Computer Security Incident Response Teams (CSIRTs), Computer Incident Response Teams (CIRTs), and/or Computer Emergency Response Teams (CERTs).
- System Architecture and Engineering**
IASAE positions are responsible for the design, development, implementation, and/or integration of an IA architecture, system, or system component.
- General User**
A user who is granted use of Government Information Systems (IS) and access to Government networks. Must complete initial and/or annual IA training as defined in the IA training BBP.
- Power User**
Personnel with roles, responsibilities, and access authorization of normal users with limited privileged-level access to that IS.
- Information Assurance Support Officer**
The Information Assurance Support Officer assist the Command's Information Assurance Manager by providing IA oversight, guidance and support to the general user in accordance with the requirements of the Command's IA Program.
- 25B/25U with Supervised Access**
A user listed with the position of 25B or 25U with Supervised Access.
- DAA**
A Senior Executive Service (SES) or a General Officer.
- DAA Representative**
A Designated Approving Authority Representative

[Next Page »](#)

- 11. QUESTIONNAIRE/DUAL STATUS:** Some personnel perform both Management and Technical duties. This requires an assignment in both the management and technical categories. If you perform duties in both categories, you will need to take this brief **questionnaire** twice.

Answer the questions first for your Primary Duty position, then on the last page select;

"**I have an additional/embedded duty**", which will allow you take this questionnaire again, answering questions for your additional/embedded duty.

You will be assigned a profile for each category...depending on your IA functions in both a primary duty and embedded duty positions. You must also select the DoD Cyberspace Workforce Frame Category, Specialty Area and Role.

1. **General Users** (example helpdesk personnel with no access to systems)
2. I have Privilege Access (**Technical Level** personnel with some or all access to an Information System residing on a Computing Environment, Network Environment or Enclave—SA/NM/NO)
3. I have **Management Responsibilities** (This is for the IASOs, IAM, IAPM, ACA, CA, and DAA)

When you complete the questionnaire, your profile assignment will appear with a link to your profile page where you may view all required training for your duty position(s)

Finished

For your Primary Duty, your assigned profile is **Technical II**. The status of your profile is unverified until a manager verified it.

Return to the [profile page](#) to view your training requirements.

“How to Login” (To old or new ATCTS accounts)

1. Type the URL or copy and paste this URL in your web browser: <https://atc.us.army.mil>
2. Click on “LOGIN” at the top right of the page or ...Click on the “LOGIN” link from the menu on the left side of the page : you will be directed to <https://atc.us.army.mil/iastar/login.php>

LOGIN SCREEN

I acknowledge and accept the above access statement.

No CAC Detected

User Name (AKO or Enterprise E-Mail Address):

Access Code:

To request an access code, [click here](#).
 For assistance with CAC related issues, [click here](#).
 If you do not have an account, please [register here](#).

* Please note that access codes may only be used once. A new code will need to be generated each time you login until your CAC is enabled for your account.

3. If you are **logging into ATCTS for the 1st time** since you registered:
 - a. You will need to retrieve your ACCESS CODE sent to the email you provided during your registration.
 - b. The login screen requires you to enter or check ;
 - i. USERNAME: The complete email address you provided during your registration
 - ii. ACCESS CODE: The code you retrieved via the email you provided during registration
 - iii. ACKNOWLEDGE: You must CHECK the box pertaining to your consent of conditions statement to access the ATCTS website
 - iv. CAC Card Enabled: This box should be checked as it pertains to your CAC being recognized by the ATCTS and therefore it is automatically associated with your ATCTS account
 - v. You must select the CAC certificate: DOD CA – 3X (the “X “ would be a number from 1 – 9)
 - vi. You must enter your CAC card PIN # to be authorized to log into your ATCTS account
 - vii. LOG IN button: Click to enter into the ATCTS Website

viii. The next time you login to ATCTS you will be able to LOGIN with your CAC Card ONLY!

“How to Login” continued

4. If you are logging into ATCTS and you do **NOT yet** have your **CAC card associated** with your ATCTS account;
 - a. You will need to retrieve your ACCESS CODE - sent to the email address on your ATCTS account by ATCTS Support or by your request at the LOGIN page, i.e. “To request an access code, [click here.](#)”



The login screen requires you to enter or check;

- i. USERNAME: The complete email address on your ATCTS account
- ii. ACCESS CODE: The code you retrieved via the email address on your ATCTS account
- iii. ACKNOWLEDGE: You must CHECK the box pertaining to your consent of conditions statement to access the ATCTS website
- iv. CAC Card Enabled: This box should be checked as it pertains to your CAC being recognized by the ATCTS and therefore it is automatically associated with your ATCTS account
- v. You must select the CAC certificate: DOD CA – 3X (the “X “ would be a number from 1 – 9)
- vi. You must enter your CAC card PIN # to be authorized to log into your ATCTS account
- vii. LOG IN button: Click to enter into the ATCTS Website
- viii. The next time you login to ATCTS you will be able to LOGIN with your CAC Card ONLY!

“How to Login” continued

- 5. If you are logging into ATCTS and you **DO have your CAC card associated** with your ATCTS account:
 - a. You must make sure your CAC Card is seated properly in the CAC reader
 - b. You must select the CAC certificate: DOD CA – **3X** (the “X “ would be a number from 1 – 9)



- c. You must enter your CAC card PIN # to be authorized to log into your ATCTS account

- 6. If you are logging into ATCTS and you **DO have an OLD CAC card associated** with your ATCTS account:
 - a. You must make sure your CAC card is seated properly in the CAC reader
 - b. You must select the CAC certificate: DOD CA – 3X (the “X “ would be a number from 1 – 9)
 - c. You will have to enter your CAC card PIN #
 - d. Your new CAC card information will be updated automatically
 - e. If your NEW CAC card has a new /different EPIPI #, then you will need to contact ATCTS Support ;
 - i. ATCTS Support will remove the OLD CAC card
 - ii. ATCTS Support will provide you with a new ACCESS CODE to associate your NEW CAC card (reference #5 above)



Users with more than one ATCTS account

Oftentimes users have **2 accounts in the ATCTS**....mainly because the AKO email system has migrated over to the Enterprise Email System. You may have registered a new ATCTS account using the new Enterprise email address, yet already have an ATCTS account with your AKO email address or even an incorrect Enterprise email address.

The ATCTS is designed for ONE ACCOUNT only for each user. Training records should be displayed in one source (the user profile) from one user account. **If any you have more than one account**, please alert ATCTS support personnel of this via a telephone **call at (816) 842-6260** or an email at support@iastar.net – which will create a support ticket in our system. Please provide you **first name, middle initial and last name also your complete email address** for all ATCTS accounts.

“How to contact FCIO for HELP”

The [contact page](#) provides phone numbers and e-mail addresses.

For assistance with Inactive Accounts, please contact your CURRENT unit IASO or IAM before dialing any numbers on the contact page

For assistance with ATCTS Website technical issues, email WillCo Technologies at support@iastar.net (Please provide your AKO or Enterprise email address with your request for assistance) or call Customer Support at (816) 842-6260. Customer support personnel are available 09:00 - 17:00 EST.

HQDA	703-697-7610 or 703-545-1703 (Army CIO/G6, Cyber Security Directorate)
106th Signal Bde	210-808-0294 (DSN 421) or 210-295-2064 (DSN 421) or 210- 295-2047 (DSN 421)
93rd Signal Bde	757-878-2497 alternate- 757-878-3254
FORSCOM	910-570-6682/7602 (DSN 670) (Cyber Security)
NGB	703-607-7059
USAR	https://esdhelp / Enterprise Email / Enterprise Customer Service Desk: 1-855-55-USARC (558-7272)
MEDCOM	210-221-7185
516th Signal Bde	808-438-1747
1st Sig Bde	DSN 315-723-2949
USAREUR	DSN 314-334-4816 COMM: +49-6132-508-816 / DSN 314-537-6196 COMM: +49-611-143-537-6196
SMDC	256-955-1802
USACE	202-761-4719
USACFSC	703-681-1579
U.S. Army North/5th Army	210-221-2096/1384 (DSN 471)
AFRICOM	DSN (314) 421-5600/2325
All Others	703-545-1703 Doris Wright or 703-697-7610 Liyla Yassin

Your ATCTS IA Training Profile – displays your current and previous training records

My Profile Page; each time you log into the system you will be directed to – My Profile page

1. How to edit info contained on your Profile Page:

My Profile

Name: **Jane Doe** (AKO: jane.doe22@us.army.mil) (Enterprise: jane.d.doe.civ@mail.mil)

Personnel Type: Military

Profile Assignment: General User (Reservist) [\[Re-Assess Profile\]](#)

Signal Command/FCIO: **U.S. Army Reserve(USAR)**-->DIVEAST (Reservist)

DRU: **U.S. Army Reserve(USAR)**-->DIVEAST (Reservist)

Assessment Date: 28/May/15

Profile Status: Unverified

[View Profile Details](#) | [Edit Account Info](#) | [View Notices \(1\)](#) | [View Unit Managers](#)

DoD Cyber Awareness Challenge Training

Click the blue i to see information about where to take this course.

Date	Type	Verified By	PDF
No DoD Cyber Awareness Challenge Training found.			

DoD 8570.01 Baseline Certifications

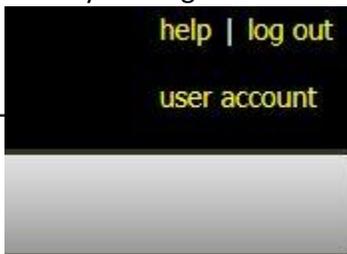
Certification	Obtained	Date	Expiration Date	Cert Num	Renewal/Enrollment	Verified	Verified By	PDF*
No certifications are required for General Users								

* - Uploading the PDF of your certificate is optional

[Add a certification](#) you have obtained.

[Add training you have completed](#)

a. You can reevaluate your profile and update the information provided during registration at any time by clicking on [I Edit Account Info](#)

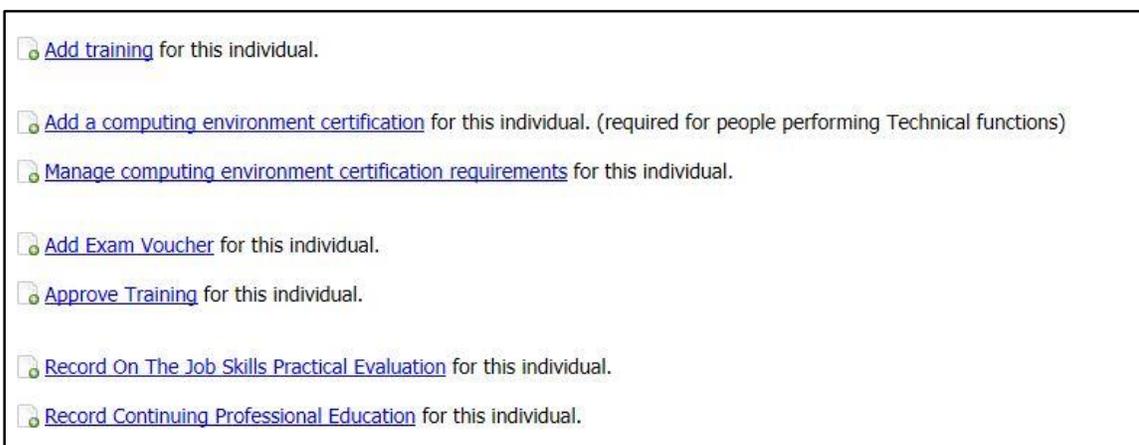


b. or you can reevaluate your profile and update the information provided during registration at any time by clicking on the [I user account](#) link that appears in the top right section of the My Profile Page

2. How to Add Training /Certification (s) to your Profile Page

The ATCTS imports training and certification completion data from Army and DOD systems such as Army E-Learning, Virtual Training website, Fort Gordon school house, DoD Virtual Training Environment (VTE) and the DoD Workforce Certification Web Application System (DWCA). (See **Online IA Training Links** below)

- a. Your AKO / Enterprise email address must be registered on all systems (Signal Center/FT Gordon, Virtual Training, Skillport and VTE) in order for your training completion records to import into your ATCTS profile.
- b. Most of your training records will be automatically imported into your ATCTS profile. However, there are some instances where you or your ATCTS manager would need to manually upload training/documentation to be visible on your ATCTS profile.
- c. My Profile Page allows you to ADD TRAINING, CERTIFICATIONS, COURSES AND DOCUMENTS



Note: Document upload must be .PDF or XFDL format and less than 2mb in size

ARMY TRAINING AND CERTIFICATION TRACKING SYSTEM USER GUIDE

Documents

The following documents should be signed, scanned, and uploaded. Uploaded files must be in PDF or XFDL format and less than 2mb in size.

Privileged Access Agreement:	<input type="text"/> <input type="button" value="Browse..."/> Date Signed: <input type="text"/> (DD/MM/YYYY) <input type="checkbox"/> NIPR <input type="checkbox"/> SIPR <input type="checkbox"/> JWICS <input type="checkbox"/> NSA <input type="checkbox"/> SAP <input type="checkbox"/> TS <input type="checkbox"/> DREN <input type="checkbox"/> CORPSNET <input type="checkbox"/> Closed Network
Duty Appointment Letters:	<input type="text"/> <input type="button" value="Browse..."/> Date of Appointment: <input type="text"/> (DD/MM/YYYY)
? Acceptable Use Policy:	<input type="text"/> <input type="button" value="Browse..."/> Date Signed: <input type="text"/> (DD/MM/YYYY)
? SAAR/DD2875:	<input type="text"/> <input type="button" value="Browse..."/> Date Signed: <input type="text"/> (DD/MM/YYYY)
** Advanced Initial Training for Military Only **	
? Advanced Initial Training (AIT):	<input type="text"/> <input type="button" value="Browse..."/> Completion Date: <input type="text"/> (DD/MM/YYYY)
? Voucher/AMF/Pretest Request Form(s)/Result(s):	New Voucher Req Doc: <input type="text"/> <input type="button" value="Browse..."/> Name of Requested Cert: <input type="text"/>
<input type="button" value="Send File(s)"/>	

How to Add Training /Certification (s) to your Profile Page: continued

- d. Based on your profile, the system will list the required/recommended certification(s) you must obtain. In regards to an Cybersecurity Technical position, you are only required to obtain one of the certifications as listed in your profile.

DoD 8570.01 Baseline Certifications

Certification	Obtained	Date	Expiration Date	Cert Num	Renewal/Enrollment	Verified	By	PDF	Modify
1 of the following certs must be obtained and verified (Technical I)									
A+	Yes	27/Sep/10	31/Dec/15	-	Cont. Ed. Enrolled - 31/Dec/12	Yes	DMDC		
A+ CE	Waived		-	-	N/A	-	-	-	N/A
CCNA Security	Waived		-	-	N/A	-	-	-	N/A
Network+	Waived		-	-	N/A	-	-	-	N/A
Network+ CE	Waived		-	-	N/A	-	-	-	N/A
SSCP	Waived		-	-	N/A	-	-	-	N/A

[Add a certification](#) for this individual.

3. How to Delete Incorrect or Outdated Training Data which should be removed

- a. If you enter incorrect dates you may delete the entry and try again
- b. Anytime you see a the **Red X** visible, you may click on to delete the date, the entry or the document

Note: In the case of the ACCEPTABLE USE POLICY document, you may have to delete a previous uploaded AUP in order to upload a new one.

ARMY TRAINING AND CERTIFICATION TRACKING SYSTEM USER GUIDE

	<input type="text" value=""/> (DD/MM/YYYY)
? Acceptable Use Policy:	01/Jun/15 View Acceptable Use Policy PDF
? SAAR/DD2875:	<input type="text"/> <input type="button" value="Browse..."/> Date Signed: <input type="text" value=""/> (DD/MM/YYYY)
** Advanced Initial Training for Military Only **	
? Advanced Initial Training (AIT):	<input type="text"/> <input type="button" value="Browse..."/> Completion Date: <input type="text" value=""/> (DD/MM/YYYY)
? Voucher/AMF/Pretest Request Form(s)/Result(s):	New Voucher Req Doc: <input type="text"/> <input type="button" value="Browse..."/> Name of Requested Cert: <input type="text"/>
<input type="button" value="Send File(s)"/>	

4. How your Profile Page gets Validated/Verified/Populated

- a. Your manager/supervisor will validate all information on your Profile Page.
- b. Training and certification information that cannot be validated through an authoritative source can be added as On the Job Training (OJT).
- c. Training/Certificates through an authoritative source which come in via the Import processes are automatically a valid record as they are populated in your profile.

5. How to Request a Token

- a. Log into your account
- b. Click on you're My Profile link located at the top of the page
- c. Scroll to the bottom of the page until you see "Request AMF Tokens"
- d. Use the pull down menu to select the token that you would like to request.
- e. Only one type of token will be provided therefore if you have a CISSP, CISM, CASP then you can only request one of those certifications for payment. All other certification fees are the responsibility of the individual.

Tokens can only be provided for appointed position. All other certification fees are the individual responsibility.

The highest CompTIA certification fee satisfies lower certification fees.

This office will only provide enough tokens to make the fees current to upload Continuing Education Credits if enough tokens are available.

Army CIO/G6 does not carry CEH or GIAC/SANS tokens. Please seek other funding avenues.

Certification	Tokens	Requested Date	Requested By
Token requests are not allowed for Contractors or State Employees.			
Security+ CE	1		<input type="button" value="Request Token(s)"/>

6. How to add the DoD Cyberspace Workforce Framework role

- a. Users will need their account unverified by the ATCTS manager first before you can reassess your profile. Once it is unverified then the user can click on reassess and start the process.
- b. Click the answer that best describes your access to the IS for your primary duty position.
- c. Click on “Next Page” located at the bottom of page
- d. Choose the answer that best describes your position or title. This refers to the categories that we currently have under DoD 8570.01-M. You can only select one item.
- e. Choose the answer that best describes your management responsibilities (CE/NE/Enclave or do not manage other personnel). This question is only available if you choose “Manager” as your access to the IS.
- f. (6) Choose the number of years you have worked in your current field.
- g. Choose your System Environment.
- h. Choose who you usually report to
- i. Click Next page.
- j. The next page opens the area to choose the work role for their position in accordance with DoDD 8140.01 and the DoD Cyberspace Workforce Framework.
- k. The first set of options are the Categories (Securely Provision, Operate & Maintain, Oversight & Development, Protect & Defend, Analyze, Operate & Collect and Investigate) specified in the DCWF. Once the category is selected then the Specialty Area will show at the bottom of the page.
- l. Select one of the specialty areas.
- m. The specialty area will expand at the bottom with the work roles. Choose at least one by clicking on the “Add Role” link. Click the “More Info” link to show all the KSAs and Tasks associated with the work role, in a separate window or tab. You only have to close it to get rid of it. You can review the Tasks and KSAs before selecting the work role. You can select up to three work roles per position/duty.
- n. Select each additional role for your primary duty by selecting another Category or a different one depending on the work role you are performing.
- o. Once you are finished adding the work roles, if needed, you may drag and drop the work roles in order from top to bottom to put them in the correct order. Primary, Secondary and Third. Click “Next” to save your work role choices and continue.
- p.). If you have an additional/embedded duty, then click the “I have an Additional/Embedded Duty” button; If you are finished adding your DCWF work roles then click on “I am Finished”.
- q. Clicking “I have an Addition/Embedded Duty” takes you back through the same path of questions that you went through for your primary duty and work role(s).

HQ Alignment Unit: **Inactivated Users**
Profile Assignment: **Technical II** [[view profile details](#)]
[8570/AR25-2] Position: System Administrator
Assessment Date: 04/Apr/13 13:14:17
Last Login Date: 04/Apr/13 13:13:04
Profile Status: Unverified

1st step

[Verify](#) [Reject](#)

Profile Assignment: **Management I** [[Re-Assess Profile](#)]
[8570/AR25-2] Position: Other Management Position
Assessment Date: 18/Aug/10
Profile Status: Unverified

2nd step

Profile Questionnaire - Page 1 3rd step

The DoD IA Workforce consists of authorized users of the Information System (IS). User access is determined by job function, the proper category, level, and function please complete this brief questionnaire. Your responses will generate a Profile for you.

* Denotes a required question.

Access

1) * Choose the answer that best describes your access to the Information System (IS) for your Primary Duty Position

Manager

A user with management or data owner access to the IS. These users would include (but are not limited to) these functional responsibility positions: IA Director, IA Deputy Director, SC/FCIO, IAPM and IAM.

Technical User

A user with system administrators (SA), IANM, or network administrator (NA) responsibilities who performs (but is not limited to) such duties as (a)Enforce the IS security guidance policies, (b)Enforce system access, operation, maintenance, or disposition requirements or (c)Review and verify currency of user accounts.

Computer Network Defense - Service Provider

A user that works with/in the Network Operations Centers (NOC), Network Operations Security Centers (NOSC), Computer Security Incident Response Teams (CSIRTs), Computer Incident Response Teams (CIRTs), and/or Computer Emergency Response Teams (CERTs).

ARMY TRAINING AND CERTIFICATION TRACKING SYSTEM USER GUIDE

1) * Choose the answer that best describes your position or title.

- CIO (Chief Information Officer)
- IAM (Information Assurance Manager)
- Alternate IAM
- IAPM (Information Assurance Program Manager)
- IANO
- ACA (Agent of the Certification Authority)
- IMO with IA Functions
- COMSEC Custodian
- COMSEC Account Manager

Management

2) * Choose the answer that best describes your management responsibilities. [\[see descriptions\]](#)

- I do not manage other IT personnel
- I manage a CE system(s)
- I manage operations for a NE
- I manage operations for an Enclave

Experience

3) * How long have you worked in Information Technology-Information Assurance or a related field?

- 0 - 4 years
- 5 - 7 years
- 8 - 10 years
- Over 10 years

System Environment

4) * Choose the answer that best describes the System Environment you work in. [\[see descriptions\]](#)

- Computing Environment
- Network Environment or Advanced Computing Environment
- Enclave Environment, advanced Network Environment, and Advanced Computing Environment

Supervision

5) * Choose the answer that best describes the level of supervision you typically operate under in your Primary duty position.

- For IA issues, typically reports to a Network Environment manager. Manages operations for a computing environment
- For IA issues, typically reports to an Enclave manager or DAA. Manages operations for a Network environment(s).
- Typically reports to a DAA or other senior level management. Manages operations for an enclave(s).

[Next Page »](#)

8140 DCWF Assessment - Page

DoD established the DCWF (DoD Cyberspace Workforce Framework) as a lexicon for the DoD cyber workforce to enable cohesive, Department-wide workforce management activities. The DCWF describes the work performed by the entire DoD cyber workforce and provides a standardized coding structure to facilitate uniform workforce identification, tracking, and reporting, as well as the development of baseline cyber workforce qualification standards.

Military and civilian personnel assigned to designated cyber positions and contractors performing cyber services must be fully qualified and identified as such in personnel management systems in accordance with DoDD 8140.01 and supporting issuances. Please use the form below to select your DCWF Category, Specialty Area and Work Role(s). You may choose up to three (Primary, Secondary and Third) DCWF work role(s) for your appointed position. When finished, Click the "Next" button.

1) * Choose the DCWF Category that best matches your Cyber Workforce position.

- General Non-Cyber [OPM Code 000]

General non-cyber specialty areas

- Securely Provision [OPM Code 060]

Specialty areas concerned with conceptualizing, designing, and building secure IT systems; responsibility for some aspect of the systems' development

2) * Choose the Specialty Area that best matches your Cyber Workforce position.

- Acquisition and Program/Project Management [OPM Code 080]

Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage a defense acquisition program. Executes duties governing hardware, software, and information system acquisition programs in the DoD Components, and other program management policies. Provides direct support for acquisitions that use information technology (IT), including National Security Systems, applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life-cycle.

- Cybersecurity Management [OPM Code 072]

Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

3) * Choose the DCWF Work Role(s) for your Cyber Workforce position

Instructional Curriculum Developer [DCWF Code 711]

Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.

[More Info](#) [Add Role](#)

* **Current Position DCWF Work Roles (drag and drop to set order, primary, secondary, third).**

Cyber Instructor [DCWF Code 712]

Develops and conducts training or education of personnel within cyber domain.

 [More Info](#)  [Remove Role](#)

Next

Finished

For your Primary Duty, your assigned 8570 profile is **Management III**. The status of your profile is unverified until a manager has verified it.

Your 8140 DCWF Work Role(s) for your Primary Duty:

1. Cyber Instructor [DCWF Code 712]

Clicking "Finished" below will take you to your profile page to view your requirements. If you have an Additional or Embedded Duty, please select that button to ta

Please select one of the following options:

or

Please upload your appointment letters to your profile within 30 days to keep this profile assignment

7. Signal Center IA Training

Fort Gordon: <https://ia.signal.army.mil> (imports INTO ATCTS every 24 hours after completion)



CYBER SECURITY TRAINING CENTER
US Army Cyber Center of Excellence Fort Gordon, GA

This is the site where you would obtain a DOD Cyber Awareness Challenge Certificate (<https://ia.signal.army.mil/DoDIAA/default.asp>) and digitally sign the AUP (Acceptable Use Policy)

For questions or issues, Email: army.ia.training@us.army.mil

Office Hours M-F 0730-1600. Allow up to 48 hours

Helpdesk (706) 791-1404

IAAT link to print certificate: <https://ia.signal.army.mil/usermngmt/linksSSO.asp>

DOD Cyber Awareness Challenge Certificate – an annual requirement



The image shows a Department of the Army Certificate of Training. At the top center is the Department of the Army seal. Below it, the text reads: "DEPARTMENT OF THE ARMY CERTIFICATE OF TRAINING". The certificate certifies that Machelie Naulty has successfully completed the "Annual DoD Cyber Awareness Challenge Exam" for 1 hour(s). The certificate was given at Fort Gordon, GA, on 17 September 2014, at the U.S. Army Signal Center. It is signed by LTC Eric Anderson. A red-bordered box at the bottom contains the following text: "The DoD 8140 reissues and renumbers DoD Directive 8570.01. It expands established policies and assigns responsibilities for managing the DoD cyberspace workforce. Signed 11 Aug 2015".

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

17 September 2014

DA Form 87, 1 Oct 78

DEPARTMENT OF THE ARMY
CERTIFICATE OF TRAINING

This is to certify that

Machelie Naulty

has successfully completed

Annual DoD Cyber Awareness Challenge Exam
1 Hour(s)

Certificate signed by LTC Eric Anderson

**The DoD 8140 reissues and renumbers DoD Directive 8570.01.
It expands established policies and assigns responsibilities for managing the
DoD cyberspace workforce. Signed 11 Aug 2015**

Notes:

- To meet Army requirements, all personnel must complete the training and score 70% or greater on the Cyber Awareness Challenge test.
- One certificate will be generated upon successful completion of the training and test. This certificate will have the SIT Director's signature preprinted on it.
- **If your certificate reads: NON-CAC: Using the NON CAC option will not transfer your certificate into your Army Training and Certification Tracking System (ATCTS) profile. ONLY use this option if you do not have a valid government issued CAC. This account is only valid for 14 days. This account and all associated training completions will be deleted on the 15th day.**

Online IA Training Links/Sites: continued

Acceptable Use Policy – an annual requirement

Acceptable Use Policy (AUP)

You must sign or digitally sign this form prior to issuance of a network userid and password. Initial Awareness Training must be completed prior to signing this agreement. IA Awareness training is found at <https://ia.signal.army.mil/dodiaa/default.asp>. The IA Awareness test located on the Fort Gordon website must be completed to fulfill the Awareness training requirement.

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

1. 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.
2. You consent to the following conditions:
 - a. 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.
 - b. At any time, the U.S. Government may inspect and seize data stored on this information system.

Acceptable Use Policy – the signature lines

21. I know that my actions as a user can greatly affect the security of the system and that my signature on this agreement indicates that I understand my responsibility as a user requires that I adhere to regulatory guidance.
22. I know I am subject to disciplinary action if I violate DOD computer policy. For U.S. personnel, this means that if I fail to comply with this policy, I may be subject to adverse administrative action or punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). If I am not subject to the UCMJ, I may be subject to adverse action under the United States Code or Code of Federal Regulations.
23. Acknowledgement: I have read the above requirements regarding use of [redacted] access systems. I understand my responsibilities regarding these systems and the information contained in them.

Computer User Name
(Last name, First, M-Rank/Grade)

(Director/Division/Branch)

Computer User
Signature

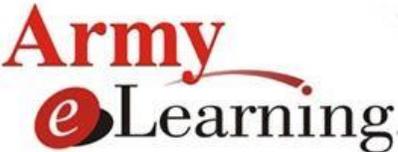
Date Signed

Online IA Training Links/Sites: continued

8. **Skillport Army e-Learning Program:** <https://usarmy.skillport.com> (imports every 48 hours after completion)

NOTE: Even though the AKO e-mail is being eliminated, your Skillport Username is still the same as your AKO Username. If you are unsure of your AKO Username, please log in to your AKO account at <https://www.us.army.mil>; click on MyAccount; choose Account Information. Your User Name is the first item listed.

- For Technical Support [Live Help](#) click here
- View a listing of the courses offered
- Access the latest FAQs



<https://usarmy.skillport.com/skillportfe/custom/login/usarmy/login.action>

For SkillSoft Technical Support Live <http://support.skillssoft.com/armyhelp/>
(CISSP Training) (866-754-5435) or 888-562-4777
Live chat: livehelp@skillssoft.com

Examples of Skillport certificates:

- No FEAR Act
- CIO G-6/NETCOM IA Technical Level 1
- CIO/G-6 NETCOM Information Assurance Security+
- CompTIA Network+
- Microsoft Windows Server 2003: Designing an Active Directory and Network Infrastructure
- CIO G6/NETCOM CISSP
- GIAC Technical Modules

9. **IA Virtual Training Website**

<https://iatraining.us.army.mil/> (imports every 24 hours after completion)



<https://iatraining.us.army.mil/usermgmt/login.htm>

For assistance, please email Customer Support at helpdesk@nacon.com or call (410) 295-5070.
Customer support technicians are available Monday-Friday 08:00-17:00 ET.
Please allow 24 to 48 hours for a response from the help desk

Online IA Training Links/Sites: continued

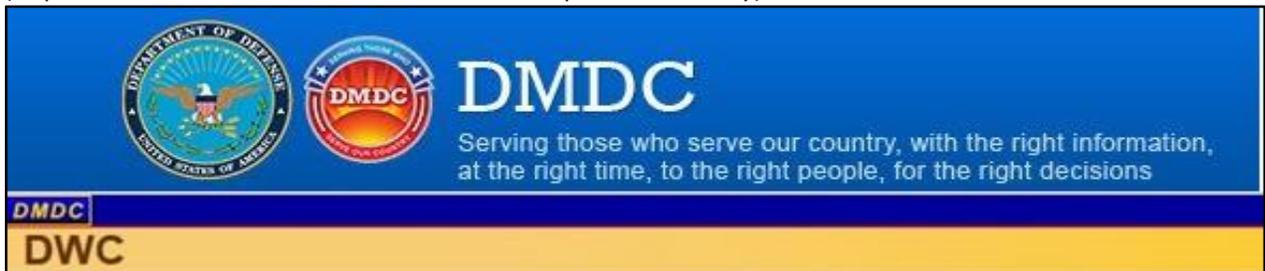
Examples of IA Virtual Training certificates: *This will satisfy Army Minimum Required Training - WNSF TRAINING*

ARMY TRAINING AND CERTIFICATION TRACKING SYSTEM USER GUIDE

- Army Specific Phishing Training
- Social Media and Operations Security
- SAFE Home Computing
- Portable Electronic Devices and Removable Storage Media
- Personally Identifiable Information (PII)
- Phishing Awareness

10. DMDC (certifications): <https://www.dmdc.osd.mil/milconnect/>

(Imports the 1st and 15th of the month- manual pulls are weekly)



The user portal to view your certs; released (from CompTia)

File Edit View Favorites Tools Help

DMDC Information and Technology for Better Decision Making

DoD Workforce Certification Application

Information Assurance Workforce

Home Authorize/Certifications Verify Email Address Contact Providers Help

Select Provider

Select the provider from which you wish to authorize the release of your certification information. Once you have authorized the release of information from a provider, any additional certifications you earn will automatically be released to the DoD. You will be notified via e-mail when any certification information is released by a provider. The email will be sent to all email addresses associated with your CAC. To view your current email information select the "Verify Email Address" tab.

Information Assurance Certification Providers

Cisco	CISCO
Compusting Technology Industry Association	CompTIA
International Council of E-Commerce Consultants	ECC
Information Systems Audit and Control Association	ISACA
International Information Systems Security Certifications Consortium	ISCC
SANS Institute	SANS
Software Engineering Institute	SEI
Security Certified Program (Inactive)	SCP

SPeD Security Professional Education Development Program

Defense Security Service (DSS) Center for Development of Security Excellence (CDSE) DSS

My Certifications

Listed below are the current certifications that you previously released to the DoD and the associated IA Category (technical or manager) and Level (1,2,3) for which the certification applies.

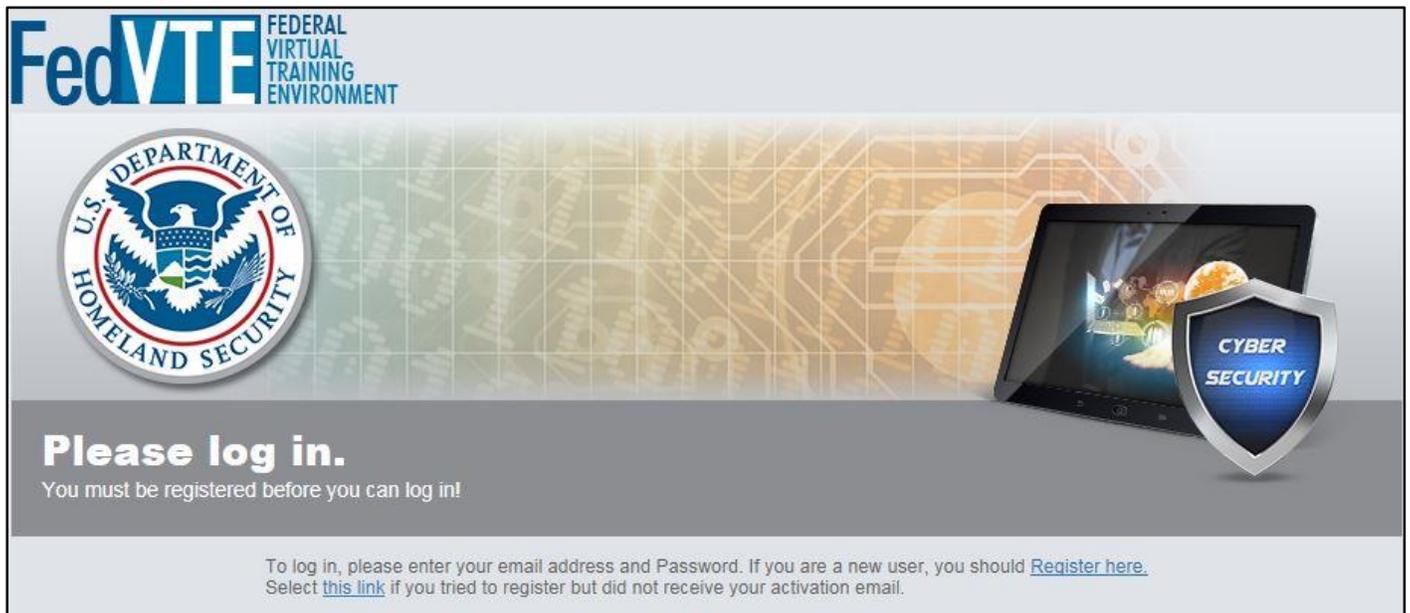
Provider	Certificate name	Issue Date	Expiration Date	Technical			Manager		
				1	2	3	1	2	3
CompTIA	Security+	02/12/2009	12/31/2012	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
CompTIA	Network+	11/30/2006	12/31/2012	<input checked="" type="checkbox"/>					
CompTIA	Security+	02/12/2009	12/31/2012	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	
CompTIA	Security+ CE	10/23/2014	10/23/2017	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	
CompTIA	Network+ CE	10/23/2014	10/23/2017	<input checked="" type="checkbox"/>					
CompTIA	Network+	11/30/2006	12/31/2012	<input checked="" type="checkbox"/>					
CompTIA	Network+ CE (Enrolled)	12/06/2012	12/06/2015	<input checked="" type="checkbox"/>					
CompTIA	Security+ CE (Enrolled)	12/06/2012	12/06/2015	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	

Indicates that the certification is valid
 Indicates that the certification has expired

COMPTIA Support: (630) – 678-8300 DMDC Support Center at 1-800-477-8227.
 The helpdesk information for DWC: 800-372-7437 (Conus) 800-538-9522 (Global)

Online IA Training Links/Sites: continued

11. **FedVTE:** <https://fedvte.usalearning.gov/> (monthly or bi-monthly depending on reports received from FedVTE helpdesk)

The banner features the FedVTE logo (FEDERAL VIRTUAL TRAINING ENVIRONMENT) in the top left, the U.S. Department of Homeland Security seal in the middle left, and a tablet displaying a globe with a 'CYBER SECURITY' shield icon in the middle right. The background is a light blue grid with faint binary code. Below the images, the text reads: 'Please log in. You must be registered before you can log in!' and 'To log in, please enter your email address and Password. If you are a new user, you should [Register here.](#) Select [this link](#) if you tried to register but did not receive your activation email.'

Examples of FedVTE certificates:

Certified Ethical Hacker

- Certified Information Security Managers/Technicians
- CompTIA A+
- CompTIA Security+ (SY0-401) Prep
- CompTIA Security+ (SY0-401)
- Cyber Risk Management for Technicians
- Cybersecurity Capability Validation Training Cybersecurity Capability Validation Training
- Certified Ethical Hacker v8
- DISA Assured Compliance Assessment Solution (ACAS)
- Linux Operating System Security
- Windows Operating System Security