

# Army CIO/G6, Cyber Security Directorate

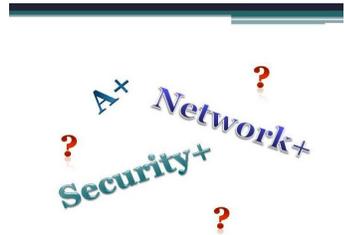
## Training and Certification Newsletter

1 February 2015



### Inside this issue:

- WHAT TO DO ABOUT EXPIRED CERTIFICATIONS IN ATCTS
- REQUESTING MOBILE TRAINING TEAM CLASSES
- FEDERAL VIRTUAL TRAINING ENVIRONMENT
- INFORMATION ASSURANCE FUNDAMENTAL TRAINING AND WORK EXPERIENCE COUNTED FOR CPES
- VALIDATION BETWEEN DMDC AND CERTIFICATION PROVIDERS SYSTEMS
- FY15 ATCTS UPGRADES
- DAILY QUESTIONS AND ANSWERS



### Points of Contact:

E-mail: Group [ciog-6.netcomiawip.inbox@mail.mil](mailto:ciog-6.netcomiawip.inbox@mail.mil)  
Phyllis.e.bailey2.civ@mail.mil  
Doris.m.wright2.ctr@mail.mil  
Ronald.m.wallace.ctr@mail.mil

# Army CIO/G6, Cyber Security Directorate

## Training and Certification Newsletter 1 February 2015

UNITED STATES ARMY

ARMY  
STRONG

### Expired and/or misrepresented baseline certifications in ATCTS

1. **The Army Training and Certification Tracking System now flags accounts with certifications that have expired.** The baseline certification percentage decreased because the AC/ASCC/DRU managers requested removal of the expired/old baseline certifications, to allow them leverage to manage accurate compliance for those with expired certifications. This process was implemented on 12 Jan 15. Here are some items that workforce personnel need to complete in order to fix their certification compliance issue.
  - a. If the expiration date is wrong in ATCTS and correct in their vendor account (comptia, ISACA, ISC(2), EC Council, SANs) then the new expiration date must be pulled into DMDC so it can be imported into ATCTS. Complete the following:
    - (1). Go to the DMDC website, <https://www.dmdc.osd.mil/appj/dwc/index.jsp> and login,
    - (2). Click on "authorized release of certification"
    - (3). Click on the vendor name of the cert you hold (the word is spelled out)
    - (4). Check " I authorize the release...."
    - (5). scroll to bottom of page and click on "release additional certifications" if your certification shows "Valid" by the "current status" then you will see the "release additional...").
  - b. If the certification has expired and the date is indeed correct in ATCTS then the individual will need to recertify to the same cert level or a higher one. However if the expiration date is less than 90 days old (comptia certs only) the individual can contact Comptia for an extension as long as they have obtained enough continuing education units (CEUs) for the cert in question.
  - c. If the individual imported the correct expiration date into DMDC and it's not showing in ATCTS because they are not annotated as an Army contractor/civilian or military in DEERS or AKO then the new certificate and their DMDC screenshot need to be uploaded into their ATCTS profile and verified by their manager so ATCTS can pick up the new date. Both the certificate and screenshot can be combined into one .pdf and uploaded under the DoD 8570.01 Baseline Certifications.
  - d. All certifications must be released through DMDC in order to receive a voucher or token (for maintenance fee payments) and all previous tokens and vouchers must be closed. If a person is annotated in AKO or DEERS as, for example- Navy reserve and Army contractor then their DMDC record will go to the Navy and not Army therefore the individual must ensure item c above is complete.

Current Matching Information			
Career ID	First Name	Middle Initial	Last Name
Current Status *	Valid		
Available Options	Release Additional Certifications		



## **Requesting Mobile Training Team classes**

1. The Army CIO/G6 has Mobile Training Teams (MTT) that provide excellent training. All students are required to test on the last day of class.
  - a. The Fort Gordon MTT, provides the following classes: CISSP (9 days), CEH (9 days), Security+ (5 days), Network+ (5 days) and CISM (5 days). The POC for class scheduling is Charmisse Owens at [charmisse.m.owens.ctr@mail.mil](mailto:charmisse.m.owens.ctr@mail.mil). You must have a minimum of 12 students (20 max) in valid cybersecurity appointed positions.
  - b. CECOM MTT provides the following classes: Digital Master Gunner (3 weeks), CISSP (9 days), CEH (9 days), CASP (9 days), A+ (9 days), CCNA Security( 9 days), CISM (5 days), Security+ (5 days), Network+ (5 days), ICNDI (5 days), ICNDII (5 days), Windows 7 (5 days), ACAS (5 days), VmWare (5 days), SCCM (5 days) and CAP (5 days). The POC for class scheduling is Stacey Garrett at [stacey.l.garrett.ctr@mail.mil](mailto:stacey.l.garrett.ctr@mail.mil) and Kenner Rodgers at [kenner.e.rodgers2.ctr@mail.mil](mailto:kenner.e.rodgers2.ctr@mail.mil). You must have a minimum of 12 students ( 16 max) in valid cybersecurity appointed positions.
2. To request a course you must provide the following items. We do not conduct MTT classes for continuing education points nor for career progression.
  - a. POC that will be accepting/rejecting registration request in ATCTS. Need name and AKO or EE mail address
  - b. Address to the training facility
  - c. City/State/Major Command of the organization
  - d. POC that will be required to help with logistic support
  - e. Address for shipping material and POC
  - f. One primary and 2 alternate dates that you wish to have the training conducted
  - g. The type of training you like to be taught
3. All on-line training (IA fundamental and skillport or FedVte) and documentation must be completed at least 2 weeks prior to the class date or the course will be canceled or rescheduled. No exceptions
4. All students are required to sign up for the class in ATCTS. Personnel not on the roster from ATCTS will not be able to attend class and be requested to leave the class if not on the roster. No exceptions.



**VERY IMPORTANT FOR ALL PERSONNEL WITH A DOD BASELINE CERTIFICATION**

All personnel: If you have a certification (ISACA/ISC(2)/Comptia/etc.) that was already released once through DMDC and the expiration date changed/renewed or a new certification was obtained then you must go back into DMDC (<https://www.dmdc.osd.mil/appj/dwc/index.jsp>) click on the vendor link that corresponds with the certification, go down to the area that shows "Current Matching Information" and click on the gray bar name "Release additional Certification". **You must complete this item each time you receive a new cert from the same vendor or have a new expiration date.**

**The Federal Virtual Training Environment Transitioning to a new platform**

The Department of Homeland Security, Cybersecurity Education and Awareness (CEA) Branch on 6 Jan 15 informed all registered users that FedVTE will shut down and move to a new platform.

During the transition all registered users must complete all training and download their completion certificates. All accounts and training will be deleted on 13 Feb 15. There is not an exact date when the new system will be accessible but the CEA Branch projects around the first week in Mar 15 if not sooner. Once the new system is accessible the Army CIO/G6 Training and Certification Branch will provide information to the community on the registration process.

The CompTIA Advanced Security Practitioner (CASP) and Certified Authorization Professional (CAP) training required for certification vouchers are the major impact on personnel since the training is not accessible through Army e-Learning. Once the new FedVTE platform is accessible, the Training and Certification Branch will provide guidance to the Cybersecurity community the registration process for the new system.



## Army CIO/G6, Cyber Security Directorate

Training and Certification Newsletter  
1 February 2015



### EXAM VOUCHERS AVAILABILITY (DA CIVILIANS AND MILITARY)



The Army CIO/G6, Cyber Security Directorate has the following vouchers and tokens available



1. CASP (tokens/ vouchers)
2. Security+ (tokens/ vouchers)
3. Network+ (tokens/ vouchers)
4. A+ (tokens/ vouchers)
5. CISM/CISA (tokens/ vouchers)
6. CISSP (tokens/ vouchers)



CEH (vouchers)- minimum number  
CCNA Security (vouchers)  
CAP (tokens/vouchers)  
ICNDI and ICNDII (vouchers)

Tokens are for the annual maintenance fees and vouchers are to take the certification exam at a commercial testing center.

Personnel outside of the 6 month appointed window must be qualified. All organizations should be at 100% compliant.

<https://iatraining.us.army.mil>  
Many DoD and Tool training.

**Helpful Websites to sustain skill sets and obtain Continuing Education credits**

<https://ia.signal.army.mil>  
-Information Assurance Fundamentals  
-DoD Cyber Challenge Awareness training  
-Mobile Training Team schedule

<https://usarmy.skillport.com> : 2500+ security and technology courses

DMDC: <https://www.dmdc.osd.mil/appj/dwc/index.jsp>

Internet Storm Center: <https://isc.sans.edu/>

DISA IASE training site: <http://iase.disa.mil/Pages/index.aspx>



## Army CIO/G6, Cyber Security Directorate

### Training and Certification Newsletter 1 February 2015



#### CERTIFICATION UPDATES

1. Security+ 401 Army E-learning training completion is required in order to request a Security+ voucher. Security+ 301 is not accepted.
2. The DoD Security+ 301 measureup must still be taken. PearsonVue is working on adding the Security+ 401 measureup test on the site: <http://dod.measureup.com> .
3. Early registration deadline for CISM/CISA June Exam is 11 February 2015 .

#### Certification Continuing Professional Education Credits

**Security:**

50 CPEs every 3 years  
\$49.00 annually

**Network+:**

30 CPEs every 3 years  
\$49.00 annually

**A+:**

20 CPEs every 3 years  
\$25.00 annually

**CASP:**

75 CPEs every 3 years  
\$49.00 annually

All GIAC: CPEs completed every  
4 years: [http://www.giac.org/certifications/  
renewal](http://www.giac.org/certifications/renewal)—  
\$100.00 annually OR 499.00 every 4 years

CISM and CISA: [http://www.isaca.org/Certification/  
Pages/maintain.aspx](http://www.isaca.org/Certification/Pages/maintain.aspx)

At least 40 per year

Total: 120 CPEs every 3 years

\$85.00 annually (non members)

\$40.00 annually (members)

CISSP: Total of 120 every 3 years

At least 40 CPEs per year

\$85.00 annual dues

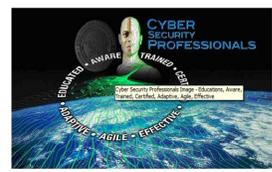
**CAP**

60 CPEs every 3 years

At least 10 CPES per year

\$65.00 annual dues

When entering CPE credits in your vendor's account (ISACA, ISC(2), etc), the CPE credit/s must align to the certification objectives.



## Army CIO/G6, Cyber Security Directorate

Training and Certification Newsletter  
1 February 2015



### DODD 8140 UPDATE

The DoDD 8140 (DoDD 8570.1 replacement) is in staffing (administrative and format correction by the DoD then legal review then for signature by the SecDef or DepSecDef. Tentative completion and release date 3rd Qtr. FY 15. New workforce manuals will be written once the Directive is signed.

The DoD Baseline Certification Chart is located at [http://iase.disa.mil/eta/iawip/content\\_pages/iabaseline.html](http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html).

### DoD Cyber Awareness Challenge training

The DoD Cyber Awareness Challenge training taken on other service's portal is acceptable for meeting the Army's requirement. The certificate from the other services' portal must be uploaded in the individual's ATCTS profile and verified by their ATCTS manager or filed in their local training folder. The training must be completed in one setting. If cookies are not turned on then the session cannot be stored.

### Information Assurance Fundamental Training Continuing Education

The 40 hour IAF training course located on the Fort Gordon website at <https://ia.signal.army.mil> counts as 40 CPE credits for the CISSP, CASP and Security+ certifications.

The training will be annotated under "Completed a Training Course" in the individual's CompTIA account.

The IA Fundamental course counts towards **16** CPE points for A+ certification and **24** CPE points for Network+

A detailed listing of skillport, FedVte and DoD courses that counts as CompTIA CPE credits are located on the ATCTS homepage under documents. Title: CompTIA CPE course **listing**.

**Remember that work history counts for 3 CPEs per year for CompTIA certified holders. Work history template is on the ATCTS homepage under documents. Work experience may be used for GIAC and other certifications as well. Please review the activity categories from your vendor's website.**



## Army CIO/G6, Cyber Security Directorate

### Training and Certification Newsletter 1 February 2015



### Validation between DMDC and the vendor site

1. The certification vendors use the following items to match the release of certifications on the DMDC website by the following items.
  - A. Candidate ID number
  - B. Name in the individual's vendor account. The name must be listed the same way on both sites.
2. If an individual full middle name is spelled out on their certificate or in their vendor account their middle name must be included with the first name when releasing through DMDC. This is the number one issue with CompTIA releases. Example: Name on certificate: John Pirate Joe. Name must be entered in DMDC

### Safari Books Online Library- another great source for security and technical books and videos

1. The DoD MWR Libraries have partnered with Safari Books Online to provide online access to the Premium Safari Books Online Library, which has over 41,208 books, videos, and tutorials.
2. These books and videos provide training on security and technical courses that can assist your Cybersecurity workforce in enhancing their skills and knowledge.
3. Access is free.
4. URL: <http://techbus.safaribooksonline.com/?uicode=dodarmy>
5. It is also accessible through AKO:
  - a. Login to AKO
  - b. click on the Self-Service dropdown link
  - c. click on My Library
  - d. click on "Read or listen to a book"
  - e. click on the Safari link
  - f. create your own login.Anyone with an AKO account can have access



## DAILY TRAINING QUESTIONS

**1. Can I upload voucher/amf request in my profile?**

**Answer:** Yes, If you are an ATCTS unit manager. If you are not then you cannot load voucher/amf request. If you are an ATCTS manager, you have to search for your name from your unit management tab. Your My profile tab treats you as a regular user.

**2. Do I have to upload my measureup pretest and where do I load it?**

**Answer:** Yes, the pretest must be uploaded in your profile and it must not be no more than 30 days old. The pretest must be uploaded in the voucher request/pretest area. Only ATCTS managers have this capability.

**3. Can I receive a voucher if I'm not in an appointed IA position?**

**Answer:** Individuals not appointed in an IA position can receive vouchers nearing expiration. The IA Program Managers will be notified 2 months prior to expiration of the vouchers that are available for distribution. Those vouchers will be provided until exhausted. Once all of the vouchers are distributed the requirements in the IA Training and Certification Best Business Practice must be adhered to for the level of certification voucher requested.

**4. How do I get my name or email address changed?**

**Answer:** If your name change from maiden to married or AKO email changed please do not create a separate account in ATCTS. Please contact Doris Wright or Ronald Wallace to assist in updating your existing account with the correct information.

**5. Who do I need to contact to assign additional ATCTS managers and deleting ATCTS managers?**

**Answer:** Contact your ATCTS of your higher command or any ATCTS manager assigned to the unit of the person that needs management rights or needs to be deleted.

**6. My Cyber Awareness Challenge training from the Fort Gordon site is not going into my ATCTS profile. Why?**

**Answer:** The import from the Fort Gordon System is currently transferred by the matching of AKO email addresses. This means that if the AKO email is not in ATCTS correctly or has been omitted then the import cannot take place. The ATCTS development team is currently working on matching by EDIPI. Personnel that takes the training by using the Non CAC feature will have to send the DISA certificate and the Army test certificate to their ATCTS manager to upload for credit.

**7. My certification is showing expired in my ATCTS profile. What do I do?**

**Answer:** Log onto DMDC site and check to see if your correct expiration date is annotated. If not then follow the instructions on page 2 of this newsletter to bring the correct date into DMDC. ATCTS pulls the results from DMDC twice weekly and updates profiles.

**8. Does Computer Network Defense Specialty positions require a technical or management appointment letter in addition to the CND appointment letter.**

**Answer:** No, only one appointment letter is required for the Specialty position. You do not need an appointment letter for IATx and CND.



**Army CIO/G6, Cyber Security Directorate**  
**Training and Certification Newsletter**  
**1 February 2015**



## Questions commands should answer regarding contracts

- Do you have contractors that perform IA support functions?
- Does their contract have the IA certification category and level requirements stated, per DoD 8570.01-M? The Performance of work (PWS) statement should state: “The contractors must comply with DFAR 252.239.7001.” Additionally you can add the DoD and Army requirements in the PWS as well.
- Is there a DD254 on file for all classified contracts or contracts that requires access to classified material?

### Contractor Certifications

**DoD DFARS 48 CFR Parts 239 and 252 RIN 0750-AF52**  
 DFARS Clause: 252.239.7001

Contractor personnel who do not have proper and current certifications shall be denied access to DoD Information Systems for the purpose of performing information assurance functions. Contractors must be hired with the required level of baseline certification as stated in their contract. The contractor has 6 months to obtain the rest of the qualification requirements unless it is stated in their contracts. (Computing Environment certification/certificate of training; Privilege Access Agreement; Duty appointment letter; background check; On-the-Job Training).

## Questions managers should answer when appointing Civilian and Military personnel to Cybersecurity positions

- Is the IA certification category and level requirement stated in the position description and the HR hiring checklist as a condition of employment?
- Is the soldier or DA civilian made aware of the type of certification/s and/or certificate of training required for their position?
- Does the supervisor mentor throughout the certification process?
- Does the supervisor counsel the individual as appropriate?

DoD 8570.01-M requires that all Department of the Army Civilians and Military personnel working IA functions obtain a baseline and computing environment certification/certificate of training within six months of their IA appointment date.



## Upcoming features for the Army Training and Certification Tracking System for FY 15

1. **Voucher Request Form** – End users may request a voucher online via the voucher request form,
2. **Voucher Request Processing** – In addition to the voucher request form, specific business processes will be put in place to help determine eligibility of personnel to receive the vouchers. The system will automatically reject requests that are not eligible. The system will send voucher requests to the designated supervisor or manager and properly add the request in the individual's profile without the need for a manual download/upload procedure.
3. **Lock/Unlock Accounts:** This feature will take the place of inactivating users when departing. The locked accounts will provide the individual access to their training page but will take the account from under the purview of the hosting organization and put it in an orphan bucket until picked up from gaining unit. All locked accounts will have the ability for managers to have a tab for Permanent Change of Station, retired, no longer at location, etc. The gaining unit will be able to search for the individual account by User ID/AKO/Enterprise E-mail address and change the status from locked to unlocked.
4. Display the latest Duty Appointment Letter on the profile but keep the letter archived which will show the date of the original letter.
5. Provide ATCTS managers a statistics dashboard for quick reviews of high-level requirements.
6. **Automatic Deactivation** – Managers will need to continually opt-in for management rights every 6 months. This allows for inactive managers to be removed automatically from the system.
7. **Community Forum** - The system will provide an area to allow members to ask questions to their respective organization or to Army CIO/G6.
8. **Assign Multiple Users** - ATCTS managers will have the ability to assign multiple users to their unit by using the individual's AKO or Enterprise email address. This will take the place of importing users via spreadsheets.
9. **Personnel Assessment** - The assessment/questionnaire will be hard coded with the functions listed in DoD 8570.01 for each category. ATCTS managers will have the ability to add additional functions as needed.