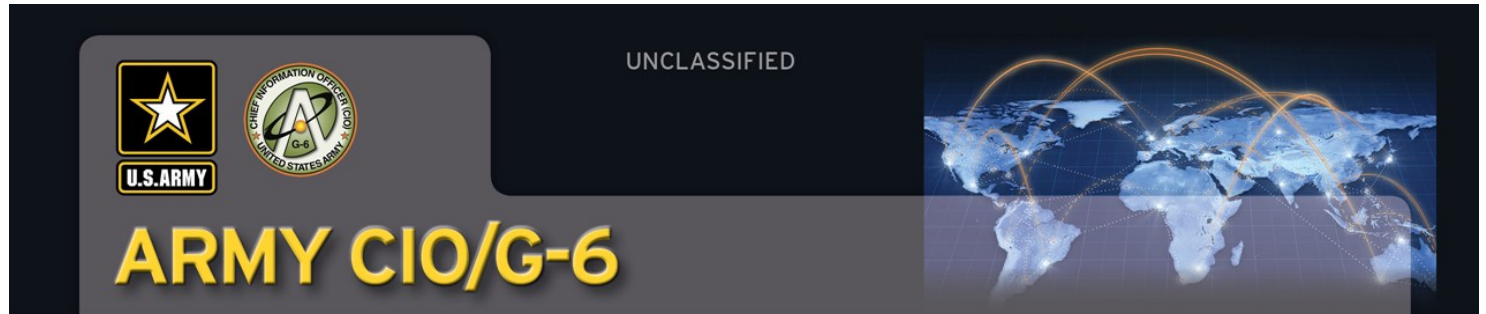
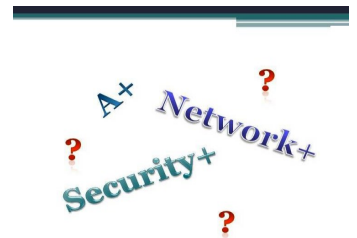


**Army CIO/G6, Cybersecurity Directorate  
Training and Certification Newsletter  
1 March 2016**



**TOPICS IN THIS ISSUE**

- GENERAL AND REGULATION (ARMY/DOD) UPDATES
- NEW FEATURES AND REGULATORY UPDATES
- INFORMATION ASSURANCE FUNDAMENTAL TRAINING AND WORK EXPERIENCE COUNTED FOR CPES
- VALIDATION BETWEEN DMDC AND CERTIFICATION PROVIDERS SYSTEMS
- FY16 ATCTS UPGRADES
- DAILY QUESTIONS AND ANSWERS
- DoD BASELINE CERTIFICATION CHART
- HOW TO RELEASE CERTIFICATION THROUGH DMDC (DWC)
- MOBILE TRAINING TEAM COURSE REQUEST REQUIREMENTS



**Points of Contact:**

Group email: [usarmy.belvoir.hqda-cio-g-6.mbx.training-and-certification@mail.mil](mailto:usarmy.belvoir.hqda-cio-g-6.mbx.training-and-certification@mail.mil)  
Phyllis.e.bailey2.civ@mail.mil  
Doris.m.wright2.ctr@mail.mil  
liyla.a.yassin.ctr@mail.mil



# Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



## GENERAL UPDATES

1. **A+ certifications:** The A+ 901 and 902 modules in skillport are scheduled to be available FY 16 2nd Qtr.
2. **Annual certification tokens must be requested annually.** If an individual owes 3 years of maintenance fees and the certification is due to expire the year the tokens are requested the Army CIO/G6 will only provide no more than 2 tokens to pay for 2 years if tokens are available. The last year payment will be the individual's responsibility. BLUF—Request tokens annually.
3. **1st time registers:** If you do not have a valid and workable Enterprise Email address please contact Liyla Yassin, 703-697-7610 or Doris Wright, 703-545-1703 for your access code. Please have a co-worker email address available to send the access code to.
4. **Skillport (Army e-Learning):** The DoD Knowledge Center has been added to skillport in the CIO/G6 /Cybersecurity IA/IT folder. The Knowledge Center comprises numerous learning resources, such as Books 24X7 reference ware, Featured Topics, and Learning Roadmaps that provide effective training. The Learning Roadmaps provide gateways to detailed instructional routes learners can take to help achieve expertise. Different roadmaps target various areas of certification and specific knowledge.
5. **DoD Cyberspace Workforce Framework (DCWF):** Personnel can review the DCWF category and Specialty Area chart in their profile. The hyperlink is under the profile assignment area.
6. The DoD Baseline Certification Chart is located at—<http://iase.disa.mil/iawip/Pages/iabaseline.aspx>.
7. **Skillport completions transferring to ATCTS:** Skillport email address must be the same as it is in ATCTS in order for courses to upload. When the address is changed in skillport please send the previous email and email address it was changed to email address: [usarmy.belvoir.hqda-cio-g-6.mbx.training-and-certification@mail.mil](mailto:usarmy.belvoir.hqda-cio-g-6.mbx.training-and-certification@mail.mil).
8. A new voucher procedure document is on the ATCTS homepage under documents. Please use this document as a guide when requesting vouchers for Cybersecurity workforce personnel. A new user guide is also available.
9. **The Cyber Awareness Challenge Version 3.0:** The training is now available on the Cybersecurity-Training Center website at <https://ia.signal.army.mil>. This training replaces the previous Cyber Awareness Challenge Version 2.0 dated Oct 2013. This update provides enhanced guidance for online conduct and proper use of information technology. 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. **The training is required every 365 days. If you took the 2.0 version and it is still current then you do not need to take the 3.0 version until the 2.0 expires.**
10. **Voucher assignment:** The Army CIO/G6, Cybersecurity Directorate purchases vouchers (for taking commercial exam) to provide to personnel in valid Cybersecurity positions. Tokens are provided to individuals that have DOD baseline certifications and need to pay their annual maintenance fees.
11. **DoD Authorizing Official (AO) Course:** The DoD AO training has replaced the previous DAA training. The AO training must be completed by all AOs every 3 years per DoD 8570.01-M. The completion certificate must be uploaded in the AO's ATCTS profile. The AO and unit training officer will sign the DAA CBT certificate upon completion. The training can be completed at <https://iatraining.us.army.mil>



# Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



## New features in ATCTS and regulation updates

### 1. DoDD 8140.01 Cyberspace Work role selection:

a. Every person in a cyberspace work role has cybersecurity responsibilities. Position description criterion will include roles identified in the DoD Cyberspace Workforce Framework (DCWF) and the cybersecurity responsibilities within each role. Contract service requirements will also be updated to include cybersecurity responsibilities for all cyberspace work roles (technical, non-technical and leadership).

b. Users logging onto the Army Training and Certification Tracking System (ATCTS) without a DCWF work role are directed to the page to add a work role. Each individual will see some information at the top of the page explaining that they need to add a work role before continuing. A DoD Cyberspace Workforce Framework power point slide is provided in each profile to assist with the selection of category and specialty areas. Please note that the DCWF work role may not be a one for one for the work role that is annotated on the appointment letter. You must choose the DCWF role that best fit your title/position.

### 2. Privileged/Elevated Access to Army Information Systems, Networks and Data:

a. LTG Ferrell (Army CIO/G6 Director) signed policy memorandum, Privileged/Elevated Access to Army Information Systems, Networks and Data on 26 Jan 2016 directing managers at all levels to review and update appointment letters, Privileged Access Agreements and roles and responsibilities for all personnel with elevated privileges. The policy memorandum directs the Network Enterprise Centers and Service Providers to evaluate all documentation for validation for access.

b. The Army Cyber Command distributed OPORD 2016-033. DTG-171450Z February 2016, It provides details about reporting and managing personnel with privileged/elevated privileges. Organizations must start evaluating accounts to make sure the DD 2875 (SAAR), appointment letters and privileged access agreement have all of the pertinent information as noted in the Policy document NLT 31 March 2016.

### 3. DoD Directive 8140.01 (Cyberspace Workforce Management), signed 11 Aug 15:

a. The Directive does not replace or reissues the DoD 8570.01-M but reissues and rennumbers DoD Directive (DoDD) 8570.01 to update and expand established policies and assigned responsibilities for managing the DoD cyberspace workforce.

b. The Directive unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements. and levels are included on all Position Descriptions.



# Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



## New features in ATCTS and regulation updates continues

c. The only changed for the Cybersecurity workforce is the selection of the DCWF role. Organization shall start ensuring that the DCWF Category, Specialty Area and role and the DoD 8570.01-M category/level is annotated in all Cybersecurity workforce ATCTS accounts.

4. **The Army Civilian Cyberspace Workforce Coding memorandum** signed by Debra Wada (Assistant Secretary of the Army, Manpower and Reserve Affairs on 10 Dec 2015) directs the review and coding of Army Civilian personnel and positions performing cyberspace work roles. Position coding provides the baseline to build viable career management solutions and enhance training to develop a ready cyberspace workforce.

Phase III of the coding effort will focus on coding civilians in the following career programs– CP11, CP16, CP19, CP34, CP35 and CP36.

## DAILY TRAINING QUESTIONS

1. **Can I upload voucher 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 Liyla Yassin 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.



**Army CIO/G6, Cybersecurity Directorate  
Training and Certification Newsletter  
1 March 2016**



**DAILY TRAINING QUESTIONS CONTINUES**

**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 on the EDIPI or AKO/EE addresses. This means that if the one of the items are not in ATCTS correctly or has been omitted then the import cannot take place. Personnel that take 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 pages 13-16 of this newsletter to bring the correct date into DMDC. ATCTS pulls the results from DMDC twice weekly and updates profiles.

**8. How do I add the date that the token or voucher was used:** **Answer:** The voucher and token section/chart in each profile is located right above the document section. The individual will click on the "ADD DATE" link located to the right of the voucher/token number. The chart is called: Your Exam Vouchers and Coupons. See below.

**9. Can contractors receive vouchers or tokens:** **Answer:** By law we cannot provide contractors or state employees vouchers or tokens.

**10. I am a reservist and contractor, can I receive a voucher or token.** **Answer:** If the certification is needed for your military position then yes as long as you have an appointment letter from your reserve organization in your ATCTS profile showing your Cybersecurity category and level. If you are not in an appointed position for the voucher or token requested then the request will be denied.

**Your Exam Vouchers and Coupons**

Exam	Vendor	Number	Auth. Code	Other Info	Date Obtained	Type	Date Used
Security+ CE 	Pearson Vue	cma567890f	-		25/Feb/16 10:12	voucher	 <a href="#">Add Date</a>

 [Add an exam voucher](#) you have obtained.

 [Record On The Job Skills Practical Evaluation.](#)

 [Record your Continuing Professional Education.](#)

**Documents**



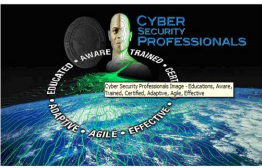
UNITED STATES ARMY

ARMY  
STRONG

## **Instructions for certifications with New Expiration Dates/Wrong Expiration dates/Not verified through DMDC**

1. log onto: <https://www.dmdc.osd.mil/milconnect/>
2. Click on "To milConnect Portal...."
3. Click on "Sign IN" located on the right side of the page, click on Login on the bottom of CAC, select your CAC certificate,
4. Click on the tab "Correspondence/Documentation pull down and select "DWCA from the pulldown menu.
5. Click on "Authorized Certifications"
6. Check the bottom of the page to see if your Certification/s is listed with the updated expiration date. IF NOT go to step "g"
7. Click on the vendor's name that your certification was issued from
8. VERY IMPORTANT: Certifications must be released each time a new expiration date is provided. If you have a valid annotation by your cert then you only have to click on the "Re Release" location under the "release" button. If you have an unknown status then go to item "9"
9. Delete any and all "UNKNOWN" status then Enter your name exactly how it is on your certificate. Enter candidate/membership ID.  
  
\*Enter name as it appears on the certificate. If the middle name is spelled out then add the middle name with the first name, leave middle initial blank then add your last name.\*
10. Once all information are entered. Check the box "I authorize the release of my certification information to 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.

**See pages 13-16 for diagrams on how to release certifications through DMDC**



Army CIO/G6, Cybersecurity Directorate  
Training and Certification Newsletter  
1 March 2016



**Certification Continuing Professional Education Credits Requirements**

**Security+:**

50 CPEs every 3 years  
\$50.00 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:**

36 CPEs completed every  
4 years:

**CISM and CISA:**

120 CPES every 3 years  
At least 40 per year  
\$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

**CEH**

120 CPEs every 3 years  
At least 40 CPES per year  
\$80.00 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. **The CCNA Security requires retest every 3 years.**

**Information Assurance Fundamental Training Continuing Education**

The 40 hour CSF training course located on the Cybersecurity Training Center website at <https://ia.signal.army.mil> counts as **40 CPE** credits for the CISSP, CASP and Security+ certifications. The training team will be updating the course between March and April to reflect more details on Risk Management Framework.

The CS Fundamental course counts towards **16** CPE points for A+ certification and **24** CPE points for Network+. Individuals should try to retake the course every 2-3 years for CPE points.

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. The 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, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



## **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), Windows Server 2012 (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). 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 the Army Training and Certification Tracking System (ATCTS). Need name and Enterprise Email 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.

5. All personnel attending the Army's MTT course must adhere to all requirements and be registered in the ATCTS. Personnel from other services that support Army and/or using the Army's network resources can take the on-line skillsoft courses on their service portal then send the completed skillsoft report to the Army's POC to upload in their ATCTS profile. Army CIO/G6 must have accountability of every person attending courses. NO EXCEPTIONS

6. MTTs are for Army Organizations that have a need to certify a large group of cybersecurity workforce personnel IAW DoD 8570.01-M. This is required by contract. Army MTTs are not provided to other DoD services and agencies. Other services and DoD agencies need to contact their Cybersecurity Division for classes.



## Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



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



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

CompTIA.



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

CCNA Security certification requires retesting every 3 years. CISCO plans to implement their continuing education program later this year. This will provide individuals the option of retesting or paying their annual fees and providing their continuing education credits in their account. Currently the number of CEUs required have not been determined.

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

FedVTE: <https://fedvte.usalearning.gov>

DMDC: <https://www.dmdc.osd.mil/milconnect>

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

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



# Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



## Upcoming features for the Army Training and Certification Tracking System for FY 16

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.



**Army CIO/G6, Cybersecurity Directorate  
Training and Certification Newsletter  
1 March 2016**



## **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 DFARS 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.



# Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016

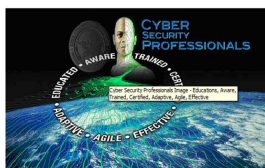


## DoD Approved 8570 Baseline Certifications

As an extension of Appendix 3 to the DoD 8570.01-Manual, the following certifications have been approved as IA baseline certifications for the IA Workforce. Personnel performing IA functions must obtain one of the certifications required for their position category or specialty and level. Refer to Appendix 3 of 8570.01-M for further implementation guidance.

Table AP3.T2 DoD Approved Baseline Certifications

IAT Level I		IAT Level II		IAT Level III	
A+-CE Network+ CE SSCP CCNA-Security		GSEC Security+ CE SSCP CCNA-Security		CISA <del>GSE</del> GCIH GCED CISSP (or Associate) CASP CE	
IAM Level I		IAM Level II		IAM Level III	
CAP <del>GISP</del> GSLC Security+ CE		CAP GSLC CISM CASP CE CISSP (or Associate)		GSLC CISM CISSP (or Associate)	
IASAE I		IASAE II		IASAE III	
CISSP (or Associate) CASP CE CSSLP		CISSP (or Associate) CASP CE CSSLP		CISSP - ISSEP CISSP - ISSAP	
CNDSP Infrastructure Support					
CNDSP Analyst		CNDSP Incident Responder		CNDSP Auditor	
GCIA CEH GCIH		SSCP CEH		GCIH CSIH CEH GCFA	
				CISA GSNA CEH	
				CISSP-ISSMP CISM	



# Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



## DoD Workforce Certification Application

Information Assurance Workforce

**Consent Notification**

This is a Department of Defense Computer System. This computer system, in management of the system, to facilitate protection against unauthorized access purposes. All information, including personal information, placed or sent over Use of this DoD computer system, authorized or unauthorized, constitutes computer purposes.

IF YOU ARE NOT AN AUTHORIZED USER, PLEASE EXIT IMMEDIATELY.

### Member (Beneficiary) Access

The Department of Defense Workforce Certification (DWC)

To milConnect Portal

step 1

### Manager & Provider Access

Manager & Provider Login

Releasing certifications through DMDC (DWCA). URL: <https://pki.dmdc.osd.mil/appj/dwc/indexWorkforceManager.jsp>

step 2

Powered by DMDC

Welcome | About milConnect | Contact Support | FAQ | Help

Welcome News FAQ

DoD Associates and Beneficiaries:

### Manage Your Personal Data and Benefits

Sign in to update personal information, like your entry in the DoD's Global Address List (GAL), or to check health care coverage, transfer education benefits, and retrieve correspondence. Sign Up to create DS Logon credentials accepted by milConnect as well as eBenefits, RAPIDS, TRICARE, and other DoD sites. Explore the milConnect FAQ for fast, accurate answers to your benefits questions, at your convenience 24/7.

### Breaking News

- February 5, 2016: Attain your goals faster in milConnect
- February 1, 2016: Request your ACA – Corrected IRS Form in milConnect
- January 9, 2016: DWC integrated in milConnect
- January 9, 2016: FSSA integrated in milConnect
- November 15, 2015: New Menus in milConnect

### Did you receive correspondence about...?

- Affordable Care Act
- Medicare and TRICARE
- Viewing PCM Information
- Retrieving eCorrespondence

Watch the milConnect Overview Video

Watch the eCorrespondence Overview Video

### Sign In

If you have a Common Access Card (CAC), DFAS (myPay) Account or DoD Self-Service (DS) Logon, click the button below to sign in.

Sign In

### Sign Up

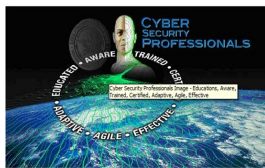
Sponsors can create a DS Logon by clicking the button below. Please have your CAC or DFAS Account ready.

Sign Up Now

### Quick Links

- Transfer Education Benefits (TEB)
- Update Address
- Update Global Address List (GAL)

Military Crisis Line



# Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



DMDC

Information and Technology for Better Decision Making



milConnect

## Self-Service Consent to Monitor

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG beneficiary self-service-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.
- While all personal identifying information (PII) data stored on this IS is protected under the Privacy Act of 1974, all communications using this IS, and the data captured to support 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.

[Contact DMDC](#) || [Accessibility/Section 508](#) || [USA.gov](#) || [No Fear Act Notice](#)

OK

## DS LOGON ?

### Department of Defense Self-Service

DS Logon Username

DS Logon Password

[Forgot DS Logon Username?](#)

[Forgot DS Logon Password?](#)

Login

## CAC ?

### Common Access Card



Login

Step 3

## DFAS myPay Password

### Defense Finance and Accounting Service

MyPay Login Id

MyPay Password

[Forgot DFAS MyPay Login Id?](#)

[Forgot DFAS MyPay Password?](#)

Login

Correspondence/Documentation

eCorrespondence

Proof of Coverage

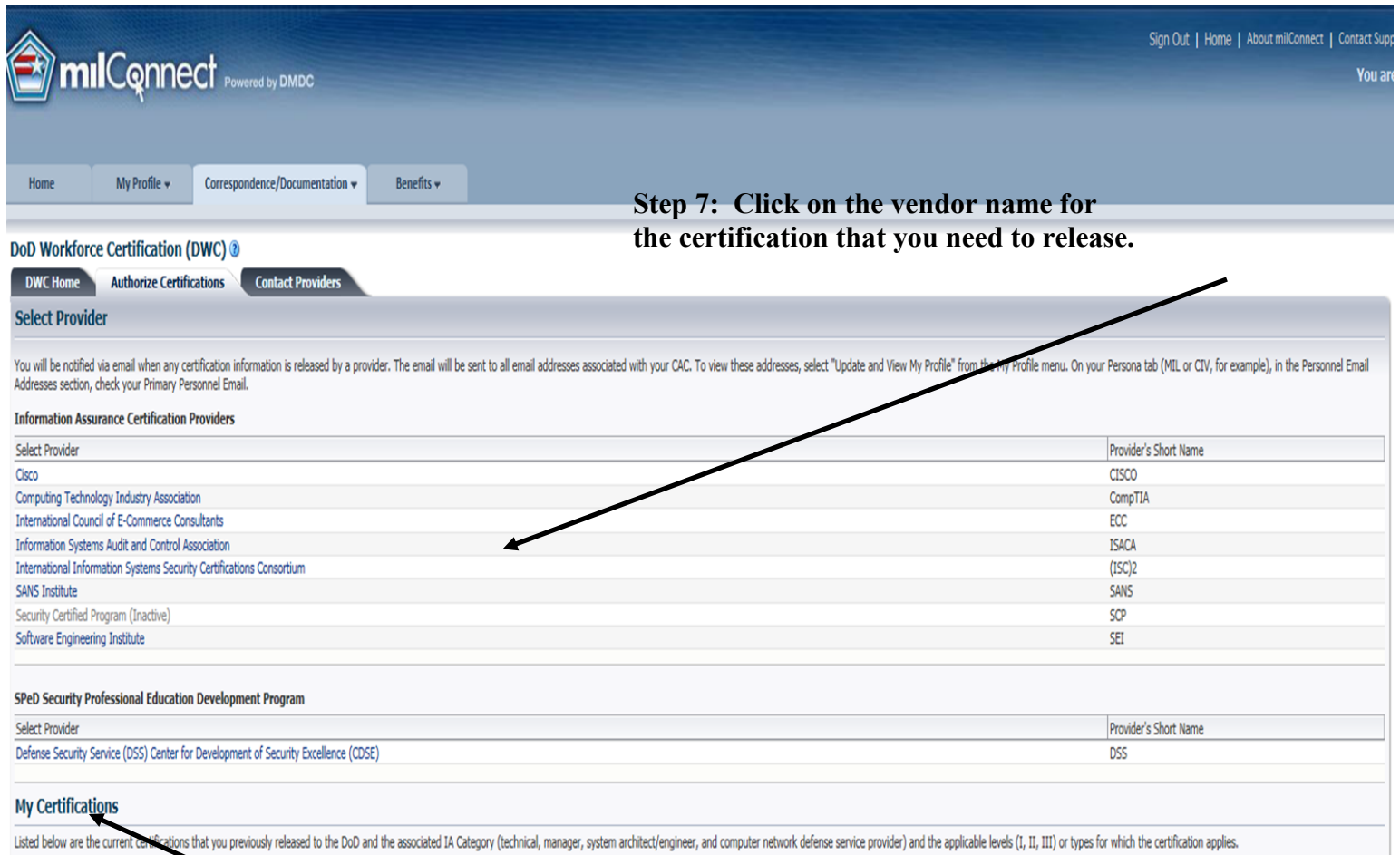
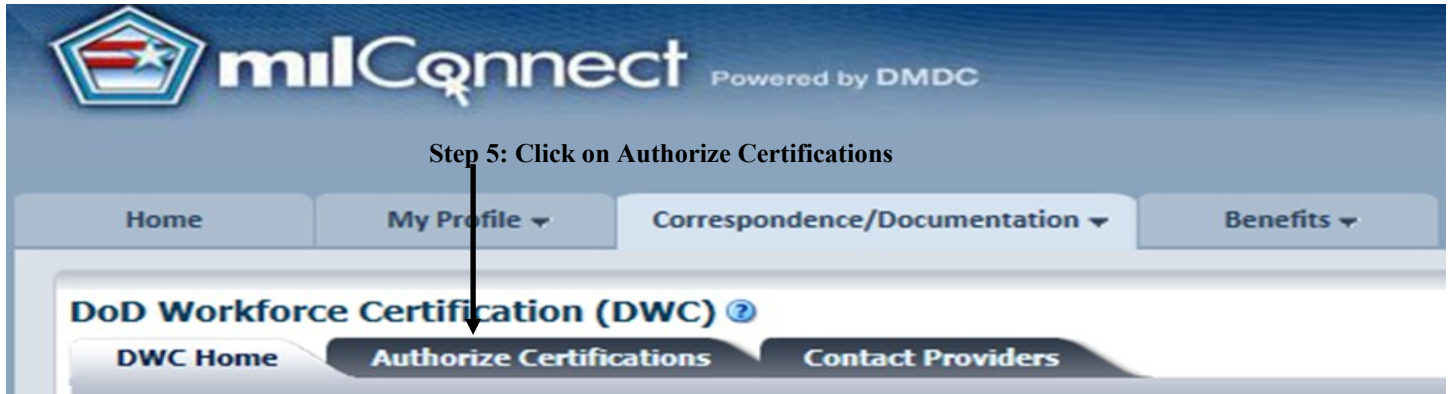
ACA - Corrected IRS Form

DoD Workforce Certification (DWC)

Step 4: hover mouse over  
“Correspondence/  
Documentation and select  
DWC



# Army CIO/G6, Cybersecurity Directorate Training and Certification Newsletter 1 March 2016



16