TRANSFORMING TALENT MANAGEMENT

DoD Chief Information Officer,
Workforce Innovation Directorate

July 2023

Agenda

- Mission Statement
- DoD CWF Strategy Implementation Plan
- Implementation Plan Timeline
- Work Roles Improve Workforce Management
- DCWF Alignment to Elements
- 8140 Qualification Program Overview
- Academic Institution Process
- Questions

CULTIVATING TOMORROW'S TALENT POOL

CWF Strategy Goal 4:

- Foster collaboration and partnerships to enhance capability development, operational effectiveness and career broadening experiences.

Objective 4.3:

- Enhance collaboration with academia to cultivate a talent pipeline and support important areas of research.

Initiative 4.3.1:

- Establish a centralized program office to manage cyber-focused student and employee developmental programs across the Department.

Initiative 4.3.2:

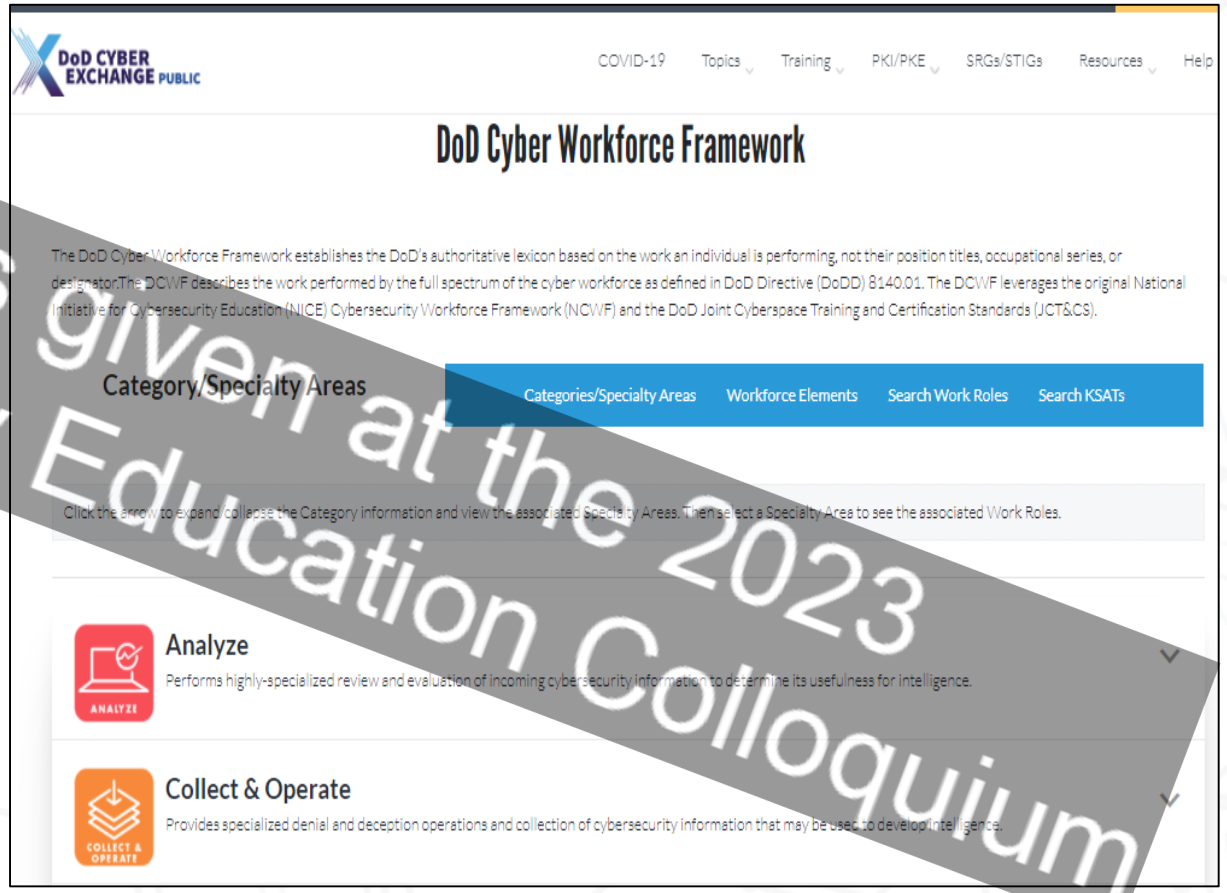
- Ensure NCAE-C curriculum aligns with Department-wide cyber standard.

Initiative 4.3.3:

- Increase return on investment of scholarship programs and effectively track participation to customize recruitment and outreach efforts.

Overview of the DoD Cyber Workforce Framework

- **What is the DCWF?**
  - Framework that serves as the DoD's standard lexicon based on the work an individual is performing, **not their position titles, occupational series, or designator**
  - It serves as the foundation for developing role-based workforce qualifications
  - Originally built for the cyberspace workforce, the DCWF **is expanding to include emerging technologies, including data, artificial intelligence, and software engineering**
- **How does the DCWF currently serve Components?**
  - Describes the work performed by the entire DoD cyberspace workforce
  - Helps DoD recruit, train, educate, and retain a qualified workforce
  - Improves interoperability throughout the DoD and with mission partners across the nation



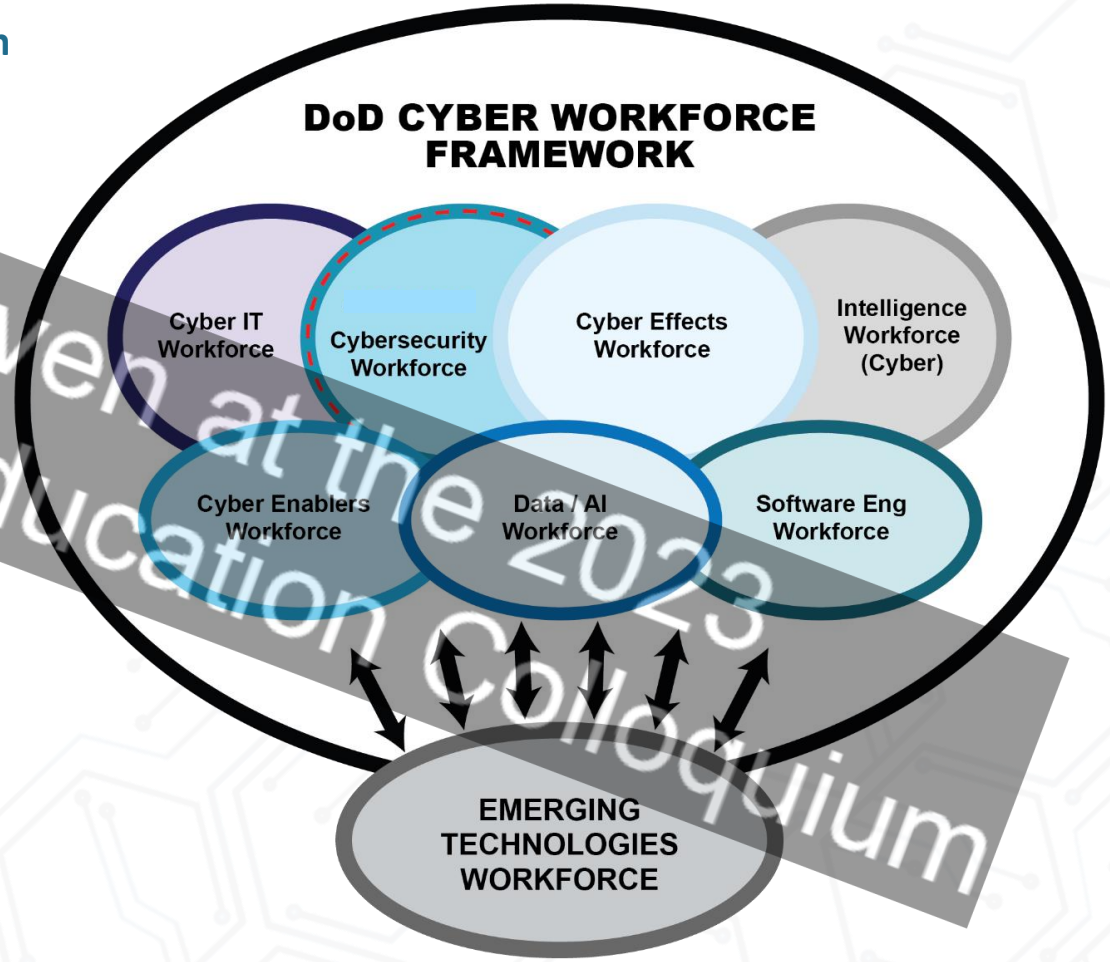
DCWF Tool Link: https://public.cyber.mil/cw/dcwf/

Work Roles Improve Workforce Management

The DoD Cyber Workforce Framework (DCWF) provides the Department with an enterprise baseline standards using Work Roles, which offer greater fidelity than historical occupational structures (e.g. civilian occupational series, military occupational specialties).

- **Agile and responsive process that can incorporate the ever-changing requirements to align to evolving technical threat landscape:**
  - Updated 39 work roles to include Cloud and DevSecOps
  - Added a Control Systems unique work role
  - The Framework now consists of 71 work roles to include Artificial Intelligence (AI), Data, and Software Engineering

- **Among it's many applications, the Department is using the DCWF to:**
  - Conduct strategic workforce planning
  - Develop tailored training and education materials
  - Qualification requirements and career progression
  - Targeted recruitment and retention incentives
  - Identification of critical recruiting and retention shortfalls (i.e., high vacancy rates & attrition rates)



DCWF Alignment to Elements

01100011 01111001 01100010 01100101 01110010 00100000 01110111 01101111 01110010 01101011 01100110 01101111 01110010 01100011 01100101 00001010

CYBER IT
OPR: DoD CIO

- (411) Technical Support Spec.
- (421) Database Administrator
- (431) Knowledge Mgr.
- (441) Network Operations Spec.
- (451) Systems Administrator
- (632) Systems Developer
- (641) Systems Requirements Planner
- (651) Enterprise Architect
- (661) Research & Development Spec.
- (671) System Testing & Evaluation Spec.

CYBERSECURITY
OPR: DoD CIO

- (212) Cyber Def. Forensics Analyst
- (511) Cyber Def. Analyst
- (521) Cyber Def. Infrastructure Support Spec
- (531) Cyber Def. Incident Responder
- (541) Vulnerability Assessment Analyst
- (611) AO/Designating Rep.
- (612) Sec. Control Assessor
- (622) Secure Software Assessor
- (631) Information Systems Sec. Developer
- (652) Security Analyst
- (722) Information Systems Sec. Mgr.
- (732) COMSEC Mgr.

CYBER EFFECTS
OPR: PCA

- (112) Mission Assessment Spec.
- (121) Exploitation Analyst
- (131) Target Developer
- (132) Target Network Analyst
- (141) Warning Analyst
- (321) Cyber Operator
- (332) Cyber Operations Planner
- (333) Partner Integration Planner

INTEL (CYBER)
OPR: USD(I&S)

- (151) Multi-Disciplined Language Analyst
- (111) All-Source Analyst
- (311) All-Source Collection Mgr.
- (312) All-Source Collection Requirements Mgr.
- (331) Cyber Intelligence Planner

DATA / AI
OPR: CDAO

- (902) AI Innovation Leader
- (733) AI Risk & Ethics Specialist
- (623) AL/ML Specialist
- (673) AI Test & Evaluation Specialist
- (753) AI Adoption Specialist
- (903) Data Officer
- (424) Data Steward
- (653) Data Architect
- (624) Data Operations Specialist
- (423) Data Scientist
- (422) Data Analyst

SOFTWARE ENG
OPR: R&E

- (621) Software Developer (update)
- (628)(New) Software/Cloud Architect
- (461) Systems Security Analyst (update)
- (627)(New) DevSecOps Specialist
- (625)(New) Product Designer User Interface (UI)
- (626)(New) Service Designer User Experience (UX)
- (806)(New) Product manager
- (673)(New) Software Test & Evaluation Specialist

CYBER ENABLERS (OPR: DoD CIO)
Support/facilitate the functions of other Cyber Workforce Categories

Leadership: (732) Privacy Compliance Mgr.; (751) Cyber Workforce Dev. & Mgr.; (752) Cyber Policy & Strategy Planner; (901) Exec. Cyber Leadership

Training & Education: (711) Cyber Instructional Curriculum Developer; (712) Cyber Instructor

Legal/Law Enforcement: (211) Forensics Analyst; (221) Cyber Crime Investigator; (731) Cyber Legal Advisor

Acquisition: (801) Program Mgr.; (802) IT Project Mgr.; (803) Product Support Mgr.; (804) IT Investment/Portfolio Mgr.; (805) IT Program Auditor

8140 Qualification Program Overview

The DoD 8140 Qualification Program establishes a **comprehensive approach** for cyber workforce talent management. It establishes Enterprise **baseline standards for qualification** that directly support operational needs and **workforce readiness**.

Key Benefits

1. Leverages and improves upon DoD 8570
2. Allows for Component customization
3. Supports integration of cyber workforce elements

DoD 8140 Qualification Program Tenets

The DoD 8140 Qualification Program was built to set cyber workforce standards for the Department while allowing for flexibility in Component implementation and workforce management.

Role-Based Progression

Qualifications are outlined based on DoD Cyber Workforce Framework (DCWF) work roles, according to three levels of proficiency, to enable career progression

Verification of Knowledge

Requisite knowledge is verified through Education or Training or Personnel Certification, providing both personnel and Components flexibility

Verification of Capability

Requisite capability is verified through On-the-Job Qualification and Environment Specific Requirements to ensure cyber personnel can meet mission needs

Continuous Professional Dev.

Personnel must complete at least 20 hours of professional development each year to ensure skillsets evolve along with changes in the environment

8140 Qualification Program Model

The DoD 8140 Manual is designed to:

- Leverage and improve upon standards established in DoD Manual 8570.
- Focus on demonstration of capability and increase flexibility for efficient implementation.
- Allow for a range of alternatives for achieving qualification.

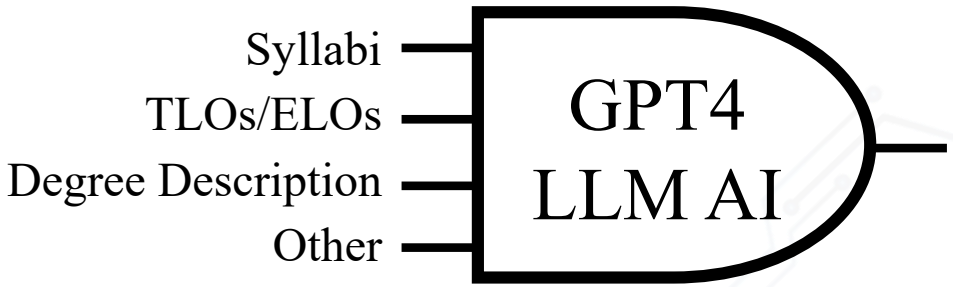
	Basic	Intermediate	Advanced
Education	Option -or- Option -or- Option	Option -or- Option -or- Option	Option -or- Option -or- Option
Training			
Personnel Certification			
On-the-Job Qualification	Always Required	Always Required	Always Required
Environment Specific Requirements	Component Discretion	Component Discretion	Component Discretion
Continuous Professional Development	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.	> Of 20 Hours/Year Or Cert. Rqmt.

8140 Qualification Model Example

(451) System Administrator				
		Basic	**Intermediate**	**Advanced**
Foundational Qualification Options	**Education**			
		OR	*OR*	*OR*
	Training	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository	Offerings listed in DoD 8140 Training Repository
		OR	*OR*	*OR*
	Personnel Certification	A+ or CND or Network+ or Security+	Cloud+ or GICSP or GSEC or SSCP	CASP+ or CCNP Security or CCSP
Foundational Qualification Alternative	**Experience**	Conditional Alternative	Conditional Alternative	Conditional Alternative
Residential Qualification	**On-the-Job Qualification**	Always Required	Always Required	Always Required
	Environment-Specific Requirements	Component Discretion	Component Discretion	Component Discretion
Annual Maintenance	**Continuous Professional Development**	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.	Minimum of 20 hours annually or what is required to maintain certification; whichever is greater.

Academic Institution Application

- Standard Operating Process developed
- Two tracks for universities applying to be added to the marketplace
  - Fast Track for those with ABET Accreditation
    - Following ACM/CSAB/INCOSE/IEEE-CS curriculum guidelines
  - Fast Track for NSA CAE Designated programs
  - Full programmatic evaluation by AI for those not meeting Fast Track rqmt
- Fast Track mapping to degree fields accomplished ahead of time by AI and SME analysis of the academic program



DoD 8140 Academic Institution Qualification Approval Process

Provider | 3rd Party Validator | Artificial Intelligence

1. Provider enters the DoD 8140 information portal.

2. Provider completes Statement of Interest survey.

3. AI reviews, provides immediate feedback, and determines next step.

4. AI notifies Provider to complete appropriate application.

5a. Provider completes and submits standard application.

5b. Provider completes fast track application.

6. AI reviews, triages, flags, and validates application.

7. 3rd Party validates application and renders decision.

7a. 3rd Party determines more information is needed. Return to block 5.

8. AI notifies Provider of decision. Case file compiled and archived.

9a. AI updates DCWF/DoD 8140 databases with awardee data.

9b. AI offers unsuccessful Providers the option to move to "Readiness Review" pool.

Academic Institution SOP Status

- Process in Beta testing
  - NDU, Citadel, CSUSB, UTSA, VT, UCF, Bowie State
  - Beta testing scheduled for completion 9/30/2023
- Six degree fields pre-mapped to DCWF work roles for ABET & NCAE programs
  - Information Systems, Information Technology, Cyber Operations, Computer Science, Data Science, Cybersecurity
- Five more degree fields in pre-mapping process
  - Computer Engineering, Electrical Engineering, Systems Engineering, Information Engineering Technology, Computer Engineering Technology
- Institutions with accounts will be notified to update their profiles as additional degree fields or other updates are made.

This presentation was given at the 2023 National Cybersecurity Education Colloquium

https://www.dodemergingtech.com/dod-cyber-workforce-qualification-program/

Survey on Cyber Education Requirements

Sponsor: Institute for Defense Analyses (IDA)
(on behalf of the DoD)

Purpose: To gather perspectives on how to best educate the DoD's cyber workforce to protect the Nation from future cyber threats (findings will be included in a report requested by Congress).

Survey Question Focus:

- Student capacity in cyber programs of study
- Educator staffing levels
- Cyber education preferences and requirements
- Perceptions of future cyber threats
- The need for a National Cyber Academy

SHARE YOUR THOUGHTS ON CYBER EDUCATION BY TAKING A BRIEF SURVEY

(visit the URL or Scan the QR Code below)

https://idaorg.gov1.qualtrics.com/jfe/form/SV_251iRbldGNIdmUC