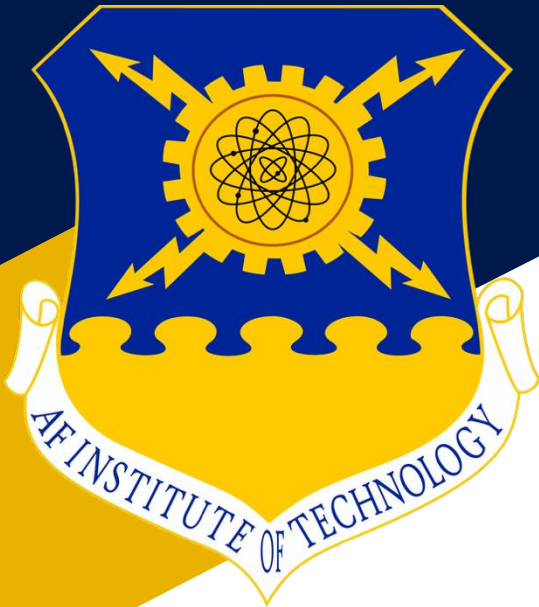




Rapid Integration of Innovative Commercial Applications for Cyber Workforce Assessments

16 July 2025

JoAnn Erno, Director, Air Force Cyberspace
Technical Center of Excellence

Mr. Ryan Vermillion, Program Manager





Motivation and Purpose



- Motivation:

- Accelerating delivery of new warfighter capabilities requires a robust infrastructure to assess the impact of change and a rapidly adaptive means of communication to ensure cyber warfighters understand the impact of that change at an ever-increasing pace of decision making.
- Competency - measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully. Competencies specify the "how" of performing job tasks, or what the person needs to do the job successfully. (<https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/>)

- Purpose:

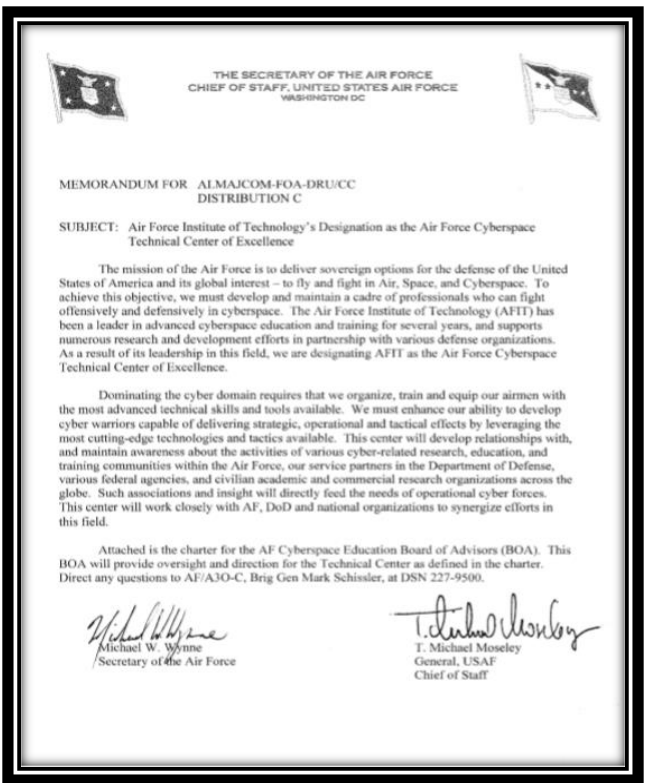
- Present a strategic approach to understanding the cyber workforce competencies to quickly deliver mission capabilities for decision superiority to the tactical edge
- Outline a framework to assess workforce competencies for strategic, operational, and tactical applications
- Discuss lessons learned and recommendations from an early implementations



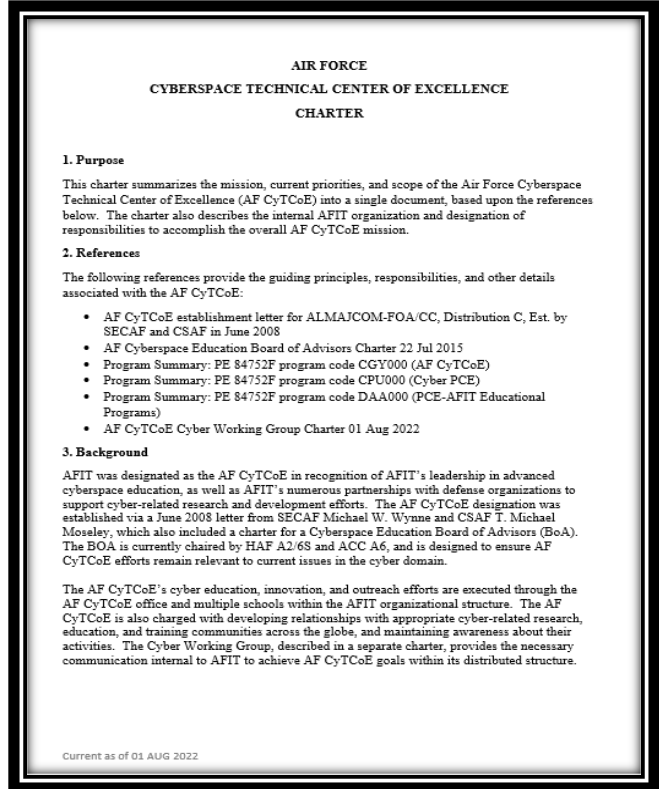
Designated as an Air Force Center in 2008 – Resident at AFIT with a Strategic Cyber Focus



2008 SecAF Center designation also established a Board of Advisors



Charter organized mission execution into Six Lines of Effort



AF CyTCoE's Purpose: To evolve the military's perspective on the changing nature of cyber warfare through innovative technology, thought leadership and partnership across operational units, government agencies and civilian academic institutions.



Defense Cyber Work Force Framework (DCWF)



- Describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01.
- Leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).
- Hierarchical structure with seven broad categories, 33 specialty areas, and 54 work roles

References:

- <https://dodcio.defense.gov/Cyber-Workforce/DCWF>
- <https://dodcio.defense.gov/Portals/0/Documents/Library/CW-StrategyImplementationPlan.pdf>

Official website of the United States government [Here's how you know](#)

CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF DEFENSE

HOME ABOUT DOD CIO LIBRARY CYBER WORKFORCE CMMC CONTACT US

Search Chief Information

FRAMEWORK

Cyber Workforce Navigation

- Overview
- DoD Cyber Workforce
 - Cyber Workforce Strategies
 - DoD Cyber Workforce Framework (DCWF)
 - Cyber Workforce Management
- Cyber Excepted Service Personnel System (CES)
- Chief Digital and AI Officer (CDAO)
- College of Information and Cyberspace (CIC)
- Cyber Service Academy (CSA)
- Cyber Information Technology Exchange Program (CITEP)
 - Info For DoD Participants
 - Info For Industry Participants
 - Useful Resources
- Resources
- Contact Us

The DoD Cyber Workforce Framework (DCWF)

Cyberspace is a warfighting domain that continues to evolve in terms of threat and complexity. As a result, the cyber workforce must also evolve to address the challenges posed by our adversaries and meet strategic mission requirements. A part of this requires reshaping our understanding of the cyber workforce to include all personnel who build, secure, operate, defend, and protect United States cyber resources; conduct cyber-related intelligence activities; and enable current and future cyber operations.

The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS). It has a hierarchical structure with seven broad categories, 33 specialty areas, and 54 work roles. Each work role contains a definition, as well as a representative list of tasks and knowledge, skills and abilities (KSAs) describing what is needed to execute key functions. Work roles vary in terms of breadth (requirements spanning multiple sets of functions) and depth (requirements focused on a related set of functions).

To increase understanding and use of the DCWF, the DoD CIO collaborated with DISA to create the DCWF Tool, an interactive online tool for stakeholders to identify, organize, and manage the tasks and KSAs of the cyberspace workforce in accordance with the DoD policy.

The DCWF Tool is available [here](#).

About DoD CIO
Contact Us
Defense.gov
DoD Careers
External Links Disclaimer
FOIA
Information Quality

No FEAR Act
Open Government
Plain Writing
Privacy Impact
Assessments
Privacy Policy
Privacy Program

Public Use Notice
Section 508
Social Media
Strategic Plan
USA.gov
Web Policy

STAY CONNECTED

f x y i m



Proposed Strategic Approach to Assess Workforce Competencies

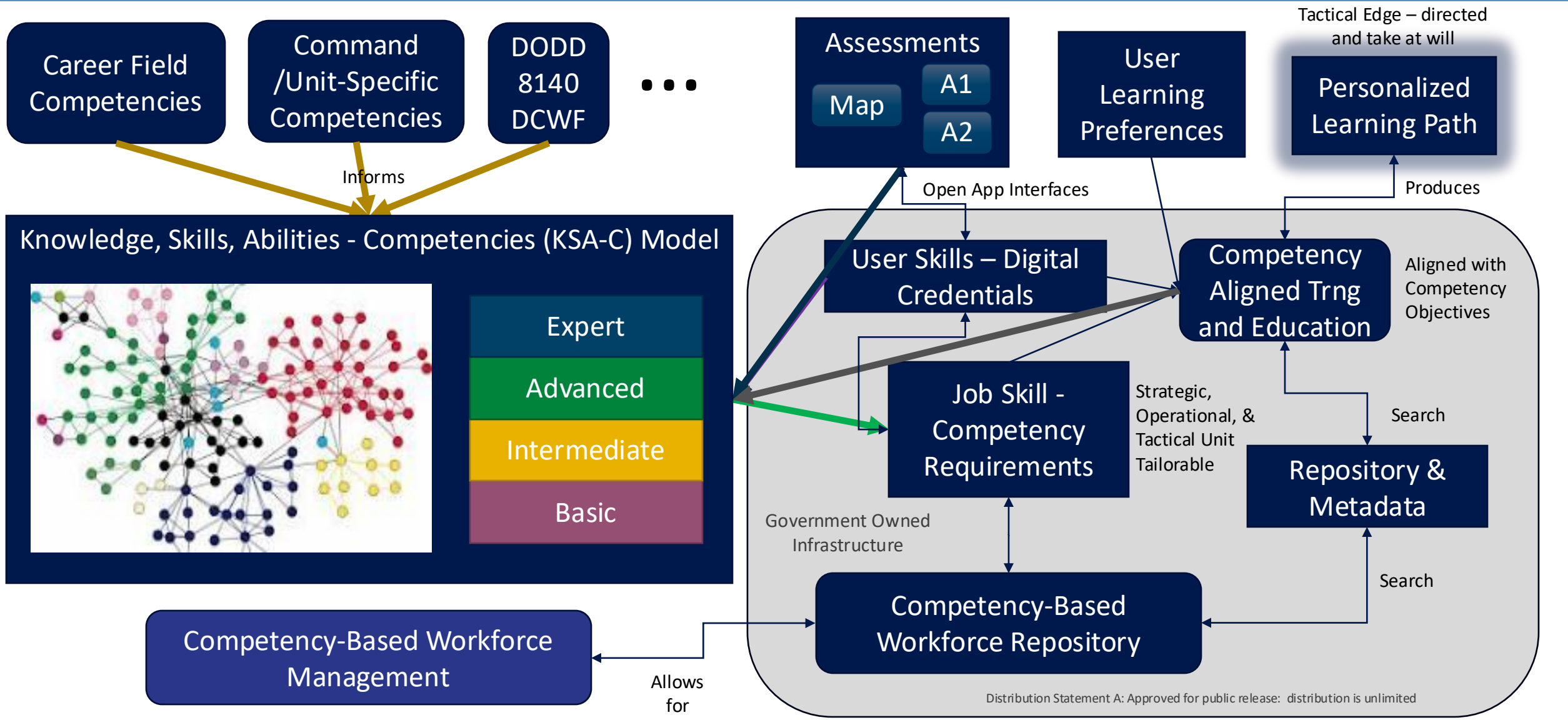


1. Maximum leverage of commercial industry for assessment technology – fast moving technology enabled by AI
2. Create a “safe place” to rapidly on-board commercial apps - no one size fits all
3. Let the “user” pick the right app for their need – leverage industry to add use cases
4. Charter an expert team to evaluate the effectiveness of different competency assessments – both from a manager and an employee perspective - government needs to own these results
5. Must maintain OPSEC to protect military capability implications – do not “aggregate” competency assessments on company “Tech Stacks”
6. Prioritize data accessibility and governance – traditional “interfaces” are not enough, need interoperable data structures to maximize effectiveness

Basic Tenets: Prioritize OPSEC while also maintaining confidentiality, integrity, availability and data accessibility



Framework for Competency Based Assessments





Lessons Learned and Recommendations



- Pace of change currently exceeds ability for government to assess and validate applications for intended use
 - Recommend an industry consortium model where products are more quickly assessed and evaluated
- Using application interfaces (via APIs) works but requires skilled manpower and time to understand and implement - okay for a research and development purpose however additional work is needed to understand multiple commercial apps use
 - Recommend additional testing to assess scalability for production ops
- Open architectures for workforce management apps needed – modularity and interoperability emphasized with distinct, interchangeable components, and common data ontologies
 - Recommend government led governance and open documentation to ensure stability and maintainability
- OPSEC – workforce competencies and aggregation of competency data potentially identifies military capability
 - Recommend ensuring all assessments anonymized when using commercial or contractor tech stacks
 - Recommend assessment data aggregation only on government secured clouds at IL-5 level to protect confidentiality
 - Recommend a government owned testing proving ground to assess validity and security of competency-based assessments
- Government owned technical baseline essential to increase efficiencies and reduce costs while also preventing vendor lock
 - Recommend government build technical depth to understand how these applications work and when to use them
- Data is the foundation of AI – AI applications require quality data sources to train, fine-tune, and sustain
 - Recommend contract language to restrict use of anonymized assessment data to government uses only for fine-tuning or updating commercial applications as additional OPSEC measures



Summary



- Robust competency assessment infrastructure needed and accessible at all levels – strategic to tactical units
- DCWF provides a cyber framework other career fields may use as a starting point
- OPSEC needs to drive framework - Government owned cloud infrastructures and tech stacks for assessment data
- Maximum use of commercial applications however Government needs to own the technical baseline to ensure agility and interoperability

Need continued investment in architectures, standards, testing and delivery of workforce competency tools to maximize cyber warfighting capability



Questions?



Air Force Cyberspace Technical Center of Excellence

- JoAnn Erno, Director, AF CyTCoE
Office: 937-713-4690
Cell: 937-475-4424
NIPR: joann.erno.2@us.af.mil (preferred)
SIPR: joann.l.erno@mail.smil.mil
JWICS: joann.erno@nasic.ic.gov
- Ryan Vermillion, CTR, AF CyTCoE Program Manager
NIPR: ryan.vermillion.ctr@us.af.mil
- Find us at:
<https://www.afit.edu/CYBER/index.cfm>

Center for Cyberspace Research

- Major Jose A. Gutierrez Del Arroyo, USAF, PhD
Director, Center for Cyberspace Research
Asst. Professor of Computer Science
Air Force Institute of Technology
COM: 937-656-4272
Email: jose.gutierrezdelarroyo.4@us.af.mil
- Major Anthony Rose, USAF, PhD
Deputy Director, Center for Cyberspace Research
Asst. Professor of Computer Science
Air Force Institute of Technology
COM: 937-656-4272
Email: anthony.rose.3@us.af.mil