"Advocating standards-based education and assessment."

Moving Forward with DoD DoD8140 Directive: Advancing Cyber Excellence

As leaders in cybersecurity, privacy, and IT upskilling, members of the C3* are pleased to support the U.S. Department of Defense (DoD) CIO Office DoD8140 Directive. We have worked for years to create, qualify, and upskill a more diverse workforce that protects United States interests, information, and infrastructure. We welcome the DoD's effort to provide clear, standards-based certification and training options, based on the 72 job roles as currently outlined in the DoD Cyber Workforce Framework site.

Certification and training options

Our C3 members have created assessment-based certification and training options that fulfill DoDDoD8140 requirements. We recognize that these options must adhere to the following standards: ISO/IEC 17024 and ANSI/ASTM E2659. All members of the C3 have been ANSI/ISO/ANAB-accredited for many years. We have decades of collective experience working with ANAB, and continue to facilitate discussions between ANAB and DoDDoD8140 directive leaders. Similarly, we work closely with the DCWF and NIST NICE. For the purposes of this document, the acronyms "ANAB," "ANSI," and "ISO," refer to effectively the same thing: Accredited training or assessment. We counsel you to avoid exceptions to these standards.

Identifying DoD8140 providers

We believe it is critical for military units and contractors to verify that the DoD8140 training and certification solutions they choose are offered by official providers that are accredited and meet ISO/ANSI standards. This step ensures that the solution you choose complies with authorized content and best practices that ensure fairness, consistency and inclusion in the upskilling and testing process. Ensuring quality is paramount.

The DoD CIO office has provided a web page called the DoD8140 Cyber Workforce Qualification Provider Marketplace. This searchable resource allows you to view all of the upskilling providers who are in the process of approval, and also who have been approved for the DoD8140 directive. C3 members offer authorized, official options for you, including the traditional certification that you have known from the superseded 8570 directive. Strongly consider choosing solutions from original, authorized providers.

Difference between training, assessment, and certification

It is important to avoid confusing the very separate activities of training, assessment, and certification.

- Training: Giving the opportunity for the workforce to learn new skills and improve performance.
- Assessment: Verifying that individuals have actually learned. Many forms of assessment exist, from traditional multiple-choice questions to cyber ranges.

Certification assures and provides confidence to DoD Leadership that all personnel that hold a valid certification have demonstrated through a legally defensible process that they have the required knowledge, skills, and attributes to perform the job. Workcred, an affiliate of ANSI, offers a detailed comparison of assessments and testing on its How Credentials Differ web page. You may also wish to consult additional resources, such as ANAB's Benefits of ANAB Accreditation page. We suggest

that you consult these resources as you plan your upskilling efforts. Certification ultimately provides unmatched skills validation for the cybersecurity community.

Nuanced options: Training, certification, and ranges

We stand ready with official offerings that validate IT skills through training and certification to U.S. troops, military personnel, and DoD contractors. We routinely develop new and performance-based certifications and training, based on market needs.

Whenever appropriate, we strive to hands-on, practical environments, adaptive learning sessions, and immersive learning activities. Each is based on industry-standard job task analysis best practices. This ensures that activities address the ever-evolving technical and threat landscape. Offerings can include, but are not limited to:

- Immersive, lab-based learning with granular reporting and validation of student achievement.
- Assessments created using AI-based data modeling and information crowdsourced from experts that meet ISO standards and lab-based testing scenarios.
- Inclusive learning and assessment solutions that attract, upskill, and retain a diverse workforce.
- Hands-on cyber ranges that provide granular skills assessment reports and foster real-time group work and contextual decision-making.
- Gamified learning that adapts intelligently to levels of competency, by job role.
- Adaptive learning that provides continuous assessment in authentic, simulated work environments, or in actual work environments

C3 members can create such offerings because we have worked closely with corporations and relevant U.S. government agencies for decades. Collectively, we have defined cutting-edge education and certification in the IT space. We continually strive to know the changing needs of the US DoD workforce.

Advocacy

It is often a challenge to create clear messaging when a new program is announced. Our members welcome the opportunity to evangelize and clarify DoD8140 in various forums and contexts. Activities can include webinars, the creation of documents and resource sites, and speaking at government and industry events (e.g., AFCEA, Billington Event, RSA). We also are available to serve as trusted advisors on the cybersecurity marketplace and workforce to US government stakeholders, Capitol Hill, and the White House.

About the C3

The Cybersecurity Credential Collaborative (C3) is a non-profit organization of the leading cybersecurity certification providers and thought leaders. Member organizations include CertNexus, CompTIA, FITSI, IAPP, ISACA, ISC2, and SANS | GIAC. Each member represents the interests of the IT, cyber, and privacy workforce. Our core mission is to help organizations around the world upskill workers using best assessment and certification standards and practices. Through advocacy, awareness, and education, C3 endeavors to ensure that cybersecurity professionals are well-equipped with the necessary skills, knowledge, and ethical grounding to navigate and secure the digital landscape.

* This document is supported by contributions from a consortium of C3 members. The insights and collaborative efforts of organizations such as CertNexus, CompTIA, FITSI, IAPP, ISACA, and SANS | GIAC have enriched the development and alignment of this document with the broader goals of cybersecurity excellence and workforce development. It is important to note that while this document benefits from the collective expertise within the C3, individual member organizations may have specific perspectives and operational priorities.