NICE FRAMEWORK SUCCESS STORY
Navy COOL and MilGears,
U.S. Navy Credentialing Programs Naval Education and Training Command

Talent Management

The voluntary Workforce Framework for Cybersecurity (NICE Framework) was developed through a collaborative process by industry, academia, and government stakeholders. It establishes a taxonomy and common lexicon that describes cybersecurity work and is intended for use in both the public and private sectors. NIST does not validate or endorse any individual organization or its approach to using the NICE Framework.

ORGANIZATIONAL PROFILE

The Office of the Deputy Secretary of Defense for Force Education and Training in the Office of the Under Secretary of Defense for Personnel & Readiness oversees the development of policies and plans for military training and education and is responsible for Service and joint training policy, cybersecurity training policy, professional military education, training capability modernization, and voluntary education, credentialing and apprenticeship policy.

DRIVERS

Procedures surrounding the qualification of the Department of the Navy (DON) Cyberspace IT/ Cybersecurity Workforce were changed in accordance with Department of Defense (DoD) Directive 8140 in coordination with the DoD Chief Information Office, Workforce Office.

This replaces DoD Directive 8570.01-M. The updated Secretary of Navy M-5239.2 establishes mandatory procedures for the uniform identification, management, and qualification of the Cyberspace IT/ Cybersecurity Workforce (Cyber IT/CSWF). All Cyber IT/CSWF personnel must meet and maintain the minimum qualification standards of their assigned Specialty Area/Work Role and proficiency level.

PROCESS

Navy COOL is a centralized, web-based hub that consolidates information from numerous sources at the federal, state, and local levels on certifications, licenses, apprenticeships, and growth opportunities that correspond with each Navy rating and Officer Designator, collateral duties, and leadership roles.

Armed with that information, COOL provides the means for Navy personnel to learn about and obtain civilian licenses and certifications that are closely aligned with their current or former military occupations, academic degrees, or civilian jobs for Reservists.
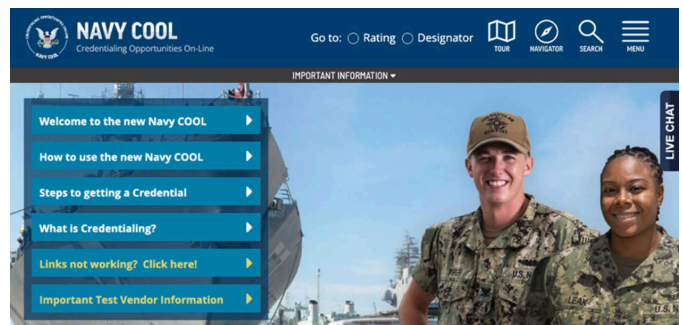

Figure 1: Navy COOL website

Navy has been and continues to the lead DoD's and the Services' COOL initiative through an effective 6-Service alliance. All the services have a COOL program, with the result being that every enlisted Military Occupational Specialty (MOS), Air Force Specialty Code (AFSC), and Navy and Coast Guard Rating are mapped to civilian occupations and at least one industry in-demand certification and/or license. Additionally, Army officers, Warrant military occupational specialties, and Navy officer designators are also mapped.

COOL is the foundation of the online platform MilGears. As the MilGears concept was developed, it was immediately recognized that it would have applicability for all the Services to use it as a career development tool that could support attainment and documentation of training, education, and experiences, as well as by other Federal departments or agencies and external organizations and industry for similar purposes. The capability to be the basis for an enterprise

course catalog was designed into the construct during the initial development phase as a consequence of requiring all source data to produce accurate and meaningful occupational pathways.

Figure 2: MilGears website

Navy next developed MilGears to support the cybersecurity workforce in line with the MilGears master development plan, mapping the Cyber/IT Workforce to the NICE Framework, the DoD Cyberspace Workforce Framework (DCWF), and assigned three-digit Governmental and Commercial Activity code for each cyber-related billet. As this has applicability to all of the Department's Cyberspace Information Technology/Cybersecurity Workforce, the Force Education and Training office is working with counterparts in the Under Secretary of Defense (Intelligence) workforce office with the Navy working directly with the other Services. The cybersecurity mapping is now live.

"While strides have been made, the language used to discuss cyber work is inconsistent. This hinders the Nation's ability to assess capabilities, identify skill gaps, and prepare the pipeline of future cyber talent. The NICE Framework gives us a source to help mitigate that."

Matthew Isnor, Program Lead,
Cyber Workforce Development, Office
of Chief Information Officer, DoD

TIE-IN WITH THE NICE FRAMEWORK

The Department of the Navy (DON) Cyberspace IT/Cybersecurity Workforce Model is based on the DoD Cyber Workforce Framework (DCWF) using the Cybersecurity Categories, and Specialty Areas, and Work Roles outlined in the National Institute of Standards and Technology (NIST) NICE Framework.

BENEFITS & IMPACT

The DoD Cyber Workforce Framework establishes the DoD's authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator. The DCWF describes the work performed by the full spectrum of the cybersecurity workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the NICE Cybersecurity Workforce Framework (NCWF) SP 800-181 and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).

CONTACT INFORMATION & RESOURCES

Contacts:

▸ Keith Boring, Director of the Navy Credentialing Programs
KEITH.BORING@navy.mil

▸ Boris Kun, Program Director, Office of the Secretary of Defense
BORIS.KUN.CIV@mail.mil

Websites:
▸ https://www.cool.navy.mil/usn/
▸ https://milgears.osd.mil/

February 2021