WILLCOTECH

Understanding the Complexities of DoD Directive 8140 / NICE vs 8570

One of the more common questions that arise in our conversations with government agencies is,

“Can you please explain the differences in DoD directive 8570 and 8140 / NICE?”

It’s a very legitimate question. Each directive has its own set of complexities and understanding the differences between them isn’t as simple and straightforward as one might think. As such, we’ve written this article to help answer exactly that. Keep reading to learn more about these directives and their differences.

DoD Directive 8570

The First in the Fight Against Cyber-Threats

Mainstream adoption of the internet happened in the United States around mid-2001when 50% of households started regularly "logging-on." It wasn't long after that cyber crime emerged.

The Department of Defense very quickly realized the risks and exposure cyber-criminals posed to our national security, so in 2005 they issued DoD directive 8570.

The main objectives of DoD directive 8570 were to:

1. Address training, certification, and management of government employees who perform information assurance (IA) or cybersecurity functions in their official assigned duties.
2. Authorize the creation (and publication) of the DoD 8570.01 manual. This manual included baseline certification requirements for those individuals working in (what is now) the cybersecurity space.

The DoD 8570 directive applied to the military, defense agencies, and government contractors working for the DoD.

It was necessary, and a great step forward in not only addressing and improving the cybersecurity posture at the time, but also learning and understanding what proficiencies and subsequent training requirements would be necessary for the cyber workforce.

While DoDD 8570 was a great start, it wasn't perfect. It left many areas unaddressed, including:

- The additional involvement of adjacent roles which heavily influenced the state of cybersecurity such as software developers
- "Level" requirements - most agencies and organizations use a matrix of roles, rather than the various "levels" of IA/cybersecurity

To address these (and many other) needs, the DoD CIO began work on DoDD 8140 / NICE.

DoD Directive 8140 / NICE

The Next Generation Directive

DoDD 8570 had acted as the backbone of cybersecurity readiness for ten years, but as the internet matured, so did the need for a revised directive. So, in 2015, the DoD CIO began work on DoD Directive 8140.01 (referred to here as simply DoDD 8140 / NICE).

DoD Directive 8140 / NICE effectively replaces DoD Directive 8570. DoDD 8570 is now part of a larger initiative that falls under the guidelines of DoDD 8140 / NICE. While the manual for 8140 / NICE is still being drafted, and the directive is not fully promulgated, it is increasingly being reviewed and showing up in requirements.

DoDD 8140 / NICE incorporates the DoD Cyber Workforce Framework (DCWF) which drew heavily from the National Initiative for Cybersecurity Education (NICE) framework, developed by none other than the National Institute of standards and technology (NIST). This is valuable because:

- The granularity of the NICE framework creates great cyber workforce opportunities, including:
  - Expanded coverage to individuals working directly in cybersecurity, or who are significant influencers into an organization's cybersecurity practices
  - Expands and adequately addresses the myriad of paths that lead to the proficiency and compliant levels for cybersecurity workers (degrees, on the job training, etc.)
- Adopts a methodology and framework that helps span from DoD through the rest of the Federal Government and into the commercial space

DoDD 8140 / NICE allows for more granular compliance and credentialing management as roles are more clearly defined.

8570 -vs- 8140 / NICE
The Differences

While DoDD 8140 / NICE (generally) expands on DoDD 8570, there are some specific differences worth noting.

1. Role organization

- DoDD 8570 has a flat structure to determine the information assurance (IA) level required
- Each level has a flat number of possible certifications or trainings required to address it

DoD Approved DoDD 8570 Baseline Certifications

IAT Level I	IAT Level II	IAT Level III
		CASP CE
	CCNA-Security	CISA
A+ CE	GICSP	CISSP (or Associate)
CCNA-Security	GSEC	GCED
Network+ CE	Security+ CE	GICSP
SSCP	SSCP	GCIH
IAM Level I	**IAM Level II**	**IAM Level III**
	CAP	
	CASP	
CAP	CISM	CISM
GSLC	CISSP (or Associate)	CISSP (or Associate)
Security+ CE	GSLC	GSLC
IASAE Level I	**IASAE Level II**	**IASAE Level III**
CASP CE	CASP CE	
CISSP (or Associate)	CISSP (or Associate)	CISSP-ISSAP
CSSLP	CSSLP	CISSP-ISSEP

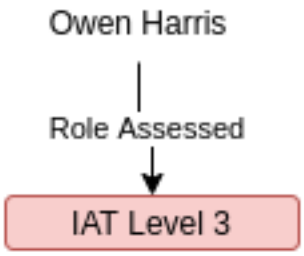
2. 8140 / NICE groups into work roles

- A work role carries with it a number of Tasks, Knowledge, and Skills statements (TKS).
- The resulting TKSs can then be collected for an individual worker
- To achieve proficiency for a given task, those Knowledge and Skills can be obtained by a large number of overlapping certifications, on the job experience, and degrees

8570 -vs- 8140 / NICE
The Differences

How to
individuals map to required training

8570
List of possible certifications for each individual
(Be careful of role changes, and the corresponding impact)



Required 1 Cert

At minimum 1 certification:
CASP CE
CISA
CISSP (or Associate)
GCED
GICSP
GCIH

1 : 1 Mapping

Required Cert Certification

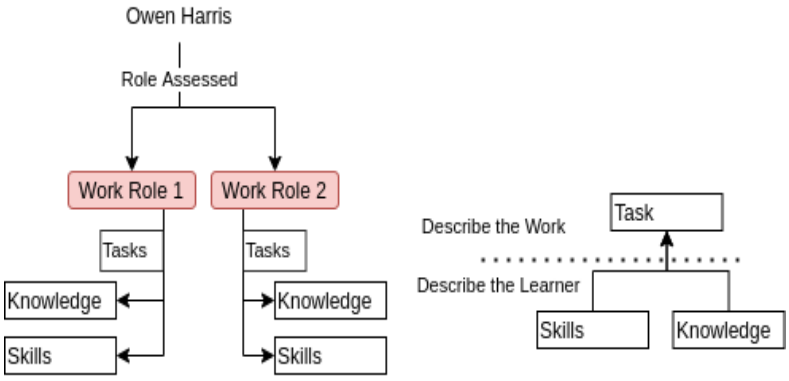
8570 -vs- 8140 / NICE
The Differences

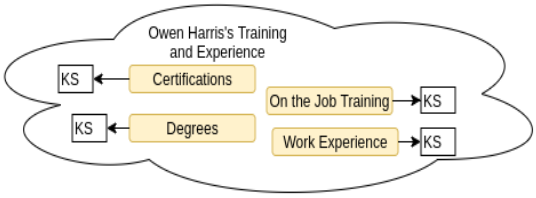
How to
individuals map to required training

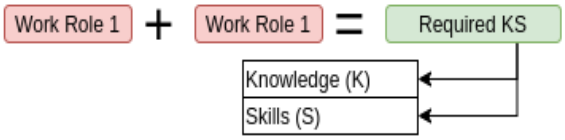
8140 / NICE
Understand the current and future roles

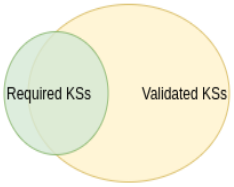
Determine the roles and tasks of the individual

** Nov 2020 - Knowledge Skills and Abilities was simplified to KS Skill statements in NIST SP 800-181r1. Competency groups, and Credentials removed for simplification of these concepts.*



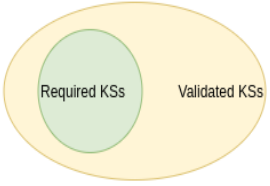






Additional Training Required

Map the Knowledge and Skills to certifications and training available



Compliant Trained and Prepared

The granularity provided by the NICE framework and acknowledging work roles is a large leap forward in truly improving cybersecurity workforce preparedness. More of the organization will require training and reporting, but it will be essential that all workers are well prepared based on their roles - as demonstrated by the ever growing number of breaches and leaks, across federal and commercial systems.

While 8570 does well to focus on required proficiency, the granularity of TKSs goes even further to enable improving the cyber workforce.

Example: An organization requires more of a particular work role

- Who is closest in their existing training overlap? Where 8570 is more akin to a 1:1 mapping or pass fail, 8140/NICE can say how close or far does a person match a role.
- What part of the organization has existing personnel if it's an emerging incident response?

How Can You Prepare?

We recommend inventorying and assessing your organization's cybersecurity teams within the NICE framework. We also suggest utilizing the roles to understand where overlap may exist as well as secondary roles individuals may have.

(816) 842-6262