WILLCOTECH

Understanding the Complexities of DOD Directive 8140 vs. 8570

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

“Can you please explain the differences between DoD Directive 8570 and 8140?”

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-2001 when 50% of households started regularly "logging-on." It wasn't long after that cybercrime emerged. The Department of Defense 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.

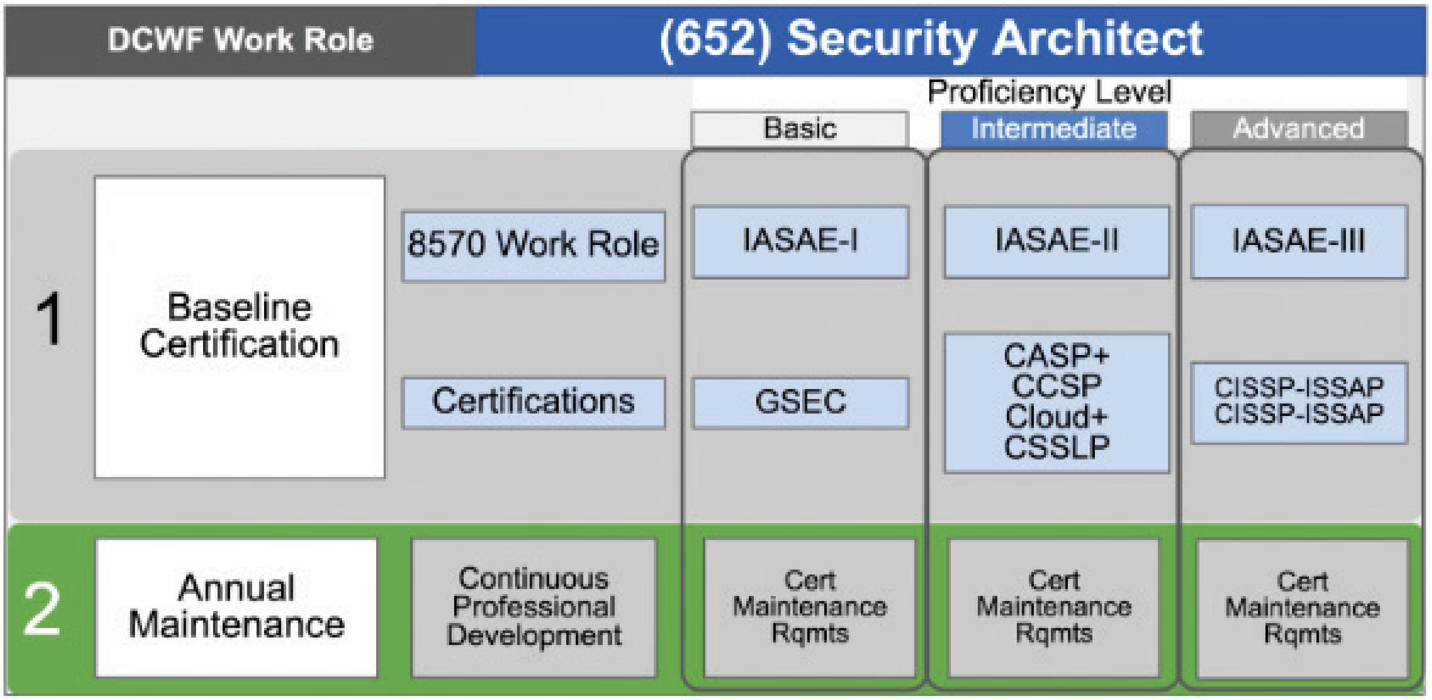
It was necessary and a great step forward in addressing and improving the cybersecurity posture at the time and learning and understanding what proficiencies and subsequent training requirements would be necessary for the cyber workforce.

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

The example below highlights the flat structure of 8570. This individual, a security architect, would need one of the applicable certifications required based on his/her proficiency level. If the person below were an IASAE-II, he would need to obtain one of the available certifications; CASP+, CCSP, Cloud+, or CSSLP.

Information Assurance - System Architects and Engineers



DCWF Work Role			(652) Security Architect		
			Proficiency Level		
			Basic	Intermediate	Advanced
1	Baseline Certification	8570 Work Role	IASAE-I	IASAE-II	IASAE-III
		Certifications	GSEC	CASP+ CCSP Cloud+ CSSLP	CISSP-ISSAP CISSP-ISSAP
2	Annual Maintenance	Continuous Professional Development	Cert Maintenance Rqmts	Cert Maintenance Rqmts	Cert Maintenance Rqmts

DoD Directive 8140

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 issued DoD Directive 8140.

DoD Directive 8140 effectively replaces DoD Directive 8570. DoDD 8570 is now part of a larger initiative that falls under the guidelines of DoDD 8140.

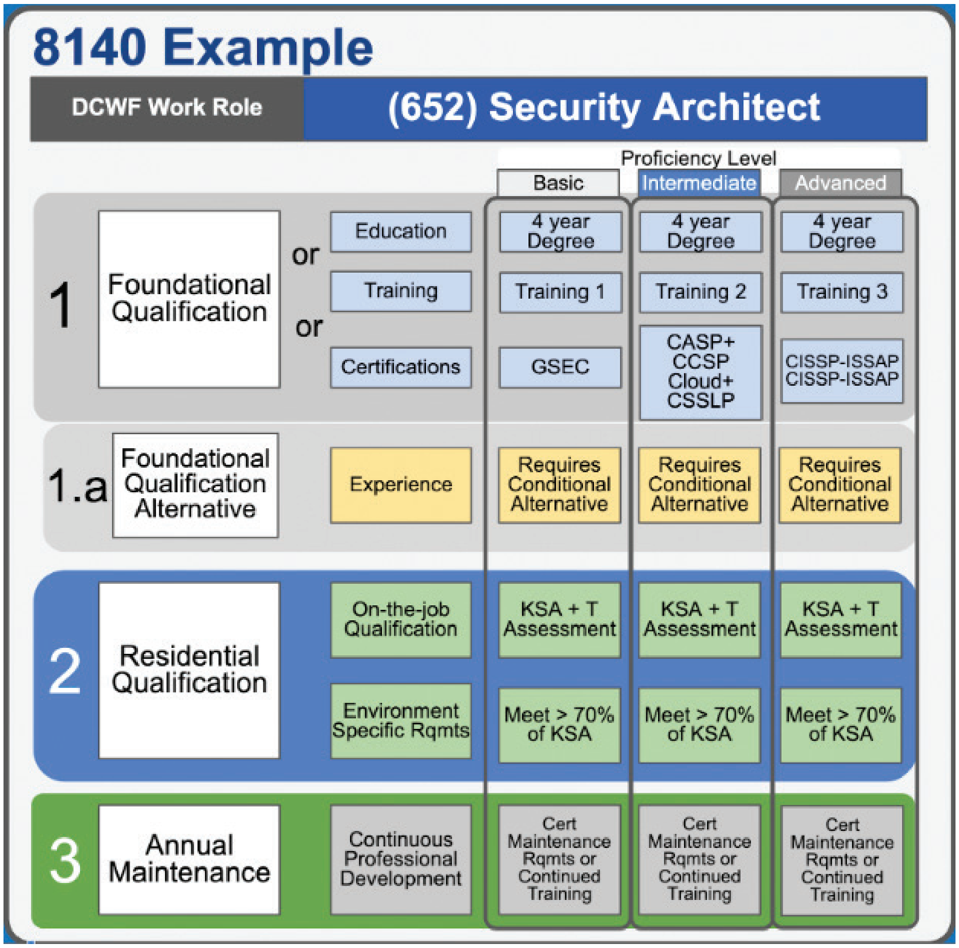
DoDD 8140 incorporates the DoD Cyber Workforce Framework (DCWF), **which draws heavily from** the National Initiative for Cybersecurity Education (NICE) framework, developed by none other than the National Institute of Standards and Technology (NIST). This is valuable because:

- 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 in an organization's cybersecurity practices
    - Expands and adequately address 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 allows for more granular compliance and credentialing management as roles are more clearly defined.

8140 / NICE groups individuals into work roles

- A work role carries with it a number of Knowledge, Skills, and Abilities (KSA)
- The resulting KSAs can then be collected for an individual worker
- To achieve proficiency, those KSAs can be covered by a large number of overlapping certifications, on the job experience, and degrees



8140 Example

DCWF Work Role | (652) Security Architect

				Proficiency Level		
				Basic	Intermediate	Advanced
1	Foundational Qualification	or	Education	4 year Degree	4 year Degree	4 year Degree
			Training	Training 1	Training 2	Training 3
		or	Certifications	GSEC	CASP+ CCSP Cloud+ CSSLP	CISSP-ISSAP CISSP-ISSAP
1.a	Foundational Qualification Alternative		Experience	Requires Conditional Alternative	Requires Conditional Alternative	Requires Conditional Alternative
2	Residential Qualification		On-the-job Qualification	KSA + T Assessment	KSA + T Assessment	KSA + T Assessment
			Environment Specific Rqmts	Meet > 70% of KSA	Meet > 70% of KSA	Meet > 70% of KSA
3	Annual Maintenance		Continuous Professional Development	Cert Maintenance Rqmts or Continued Training	Cert Maintenance Rqmts or Continued Training	Cert Maintenance Rqmts or Continued Training

DoD Directive 8140

The Next Generation Directive

In February 2023, the Department of Defense released the DoD Manual 8140.03, "Cyberspace Workforce Qualification and Management Program." The manual provides guidance and procedures for managing and developing the DoD's cyberspace workforce, covering a wide range of topics related to cyberspace workforce management.

The manual requires agencies and contractors to have cyber positions and roles mapped, analyze proficiency requirements with DoD Instruction 8140.02, provide data on the current force in accordance with 8140.02, and appropriately resource cyber qualification requirements and workforce management systems.

Specific requirements within 12 months of the manual's effective date include

- identifying all positions designated as cyberspace workforce positions
- analyzing all cyberspace workforce positions to ensure a proficiency level is assigned in accordance with DoD Instruction 8140.02
- and providing data on incumbent cyberspace workforce positions to the Defense Manpower Data Center (DMDC).

Within two years of the effective date of the manual, all DoD civilian employees and Service members in cyberspace work roles under the cybersecurity workforce element must be qualified in accordance with this issuance.

Within three years of the effective date, all DoD civilian employees and service members in work roles under the cyberspace IT, cyberspace effects, intelligence (cyberspace), and cyberspace enabler workforce elements must be qualified in accordance with this issuance. Contractors must be qualified in accordance with this issuance at the commencement of work.

8570 vs. 8140

The Differences

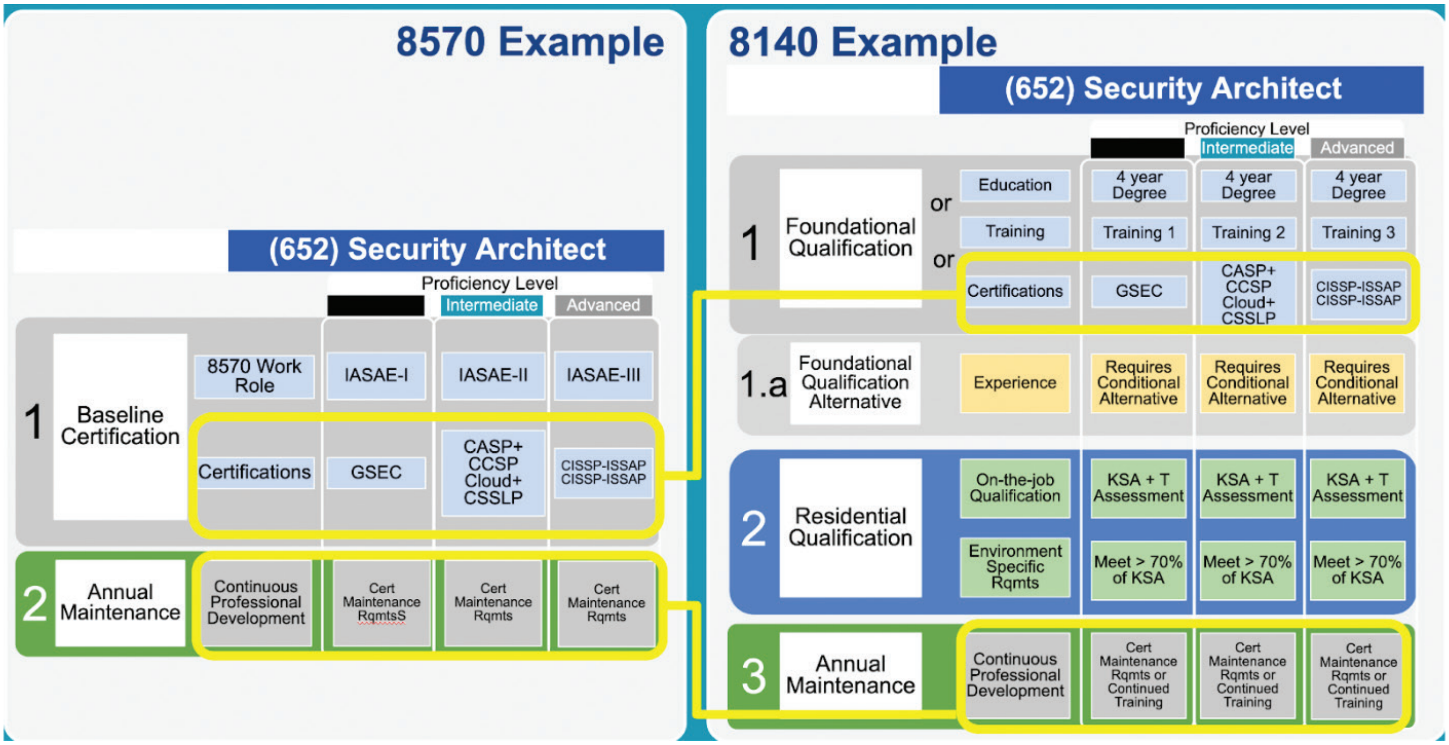
DoD Directive 8570 required training, certification, and management of government employees who perform information assurance (IA) or cybersecurity functions in their officially assigned duties.

In contrast, DoD Directive 8140 dramatically expands complexity, identifying 71 work roles with 3 proficiency levels, each equaling 213 unique work roles. This increased granularity leads to a role mapping that is much more closely aligned to what the individual is actually performing.

Qualifications are now defined via matrices that Include:

- **Foundational Qualifications** (Education OR Certification OR Training OR Assessment)
- **Residential Qualifications** (per-component training, OJT, computing environments)
- **Continuing Education Qualifications** (CPEs, cert renewals)
- **Grouped by Workforce Element** (10 defined) - no Longer Using Categories or Specialty Areas

The example below shows a side by side comparison of 8570 and 8140 using the same security architect role.



8570 Example

(652) Security Architect

			Proficiency Level		
			[redacted]	Intermediate	Advanced
1	Baseline Certification	8570 Work Role	IASAE-I	IASAE-II	IASAE-III
		Certifications	GSEC	CASP+ CCSP Cloud+ CSSLP	CISSP-ISSAP CISSP-ISSAP
2	Annual Maintenance	Continuous Professional Development	Cert Maintenance RqmtsS	Cert Maintenance Rqmts	Cert Maintenance Rqmts

8140 Example

(652) Security Architect

				Proficiency Level		
				[redacted]	Intermediate	Advanced
1	Foundational Qualification		Education	4 year Degree	4 year Degree	4 year Degree
		or	Training	Training 1	Training 2	Training 3
		or	Certifications	GSEC	CASP+ CCSP Cloud+ CSSLP	CISSP-ISSAP CISSP-ISSAP
1.a	Foundational Qualification Alternative		Experience	Requires Conditional Alternative	Requires Conditional Alternative	Requires Conditional Alternative
2	Residential Qualification		On-the-job Qualification	KSA + T Assessment	KSA + T Assessment	KSA + T Assessment
			Environment Specific Rqmts	Meet > 70% of KSA	Meet > 70% of KSA	Meet > 70% of KSA
3	Annual Maintenance		Continuous Professional Development	Cert Maintenance Rqmts or Continued Training	Cert Maintenance Rqmts or Continued Training	Cert Maintenance Rqmts or Continued Training

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

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 the secondary roles individuals may have.

Our CyberSTAR™ platform is engineered as a complete solution for FISMA, DoD 8570, and DoD 8140 requirements (DCWF). It comes off-the-shelf and is able to automate the ingestion and validation of thousands of training and qualification records, allowing CyberSTAR™ to map and maintain a continuous report against the 8140.03M qualification matrix: offering a clear and actionable picture to the organization from the individual, through all reporting echelons, to leadership. Additionally, CyberSTAR™ can directly integrate with your existing Active Directory and LMS systems.

CyberSTAR™ automates the monitoring, management, and alerting for cyber workforce credentials and compliance and is the only DoDD 8140-compliant platform contracted for use within the Department of Defense.

1. Through HR system integration, manual mapping, or an online assessment tool, individuals can be identified and mapped to their proper category and level. A profile is given to each system user - whether civilian, service member, or contractor.
2. Courses from DoD entities or commercial training vendors can be loaded into the CyberSTAR™ system. The system auto-generates a training plan with the relevant courses needed for workforce compliance. Courses can also be launched from the platform.
3. Certification exam vouchers can be imported, distributed, and managed. E-vouchers are assigned to users that are ready to take the exam. A voucher distribution system manages the process using a voucher-on-demand model.
4. Multiple reports can be generated at every system hierarchy level.

Compliance data can be retrieved, and reports generated at any time. Your organization can set compliance parameters and results placed in the proper database.

WILLCOTECH

(816) 842-6262