



TIER ONE TALENT & INTEL RECRUITING

Mission-Ready Talent. Defense-Built Solutions.

DoD CYBER WORKFORCE

DCWF, DoDM 8140.03, and Your Certification Path

UPDATED MAY 2026 • VERSION 2.0

DoD cyber workforce policy has fundamentally changed. The old **DoD 8570.01-M** framework with its IAT / IAM Level I, II, and III categories was officially cancelled on February 15, 2023. The successor — **DoD Manual 8140.03** — replaces broad certification "levels" with a role-based qualification model under the DoD Cyber Workforce Framework (DCWF).

WHAT CHANGED

- **DoD 8570.01-M Cancelled** Officially superseded by DoDM 8140.03 on February 15, 2023. The IAT and IAM Level I, II, and III categorization is no longer the operative framework.
- **Role-Based, Not Level-Based** Qualifications now map to specific DCWF work roles (70+ total across 7 workforce elements), each with Basic, Intermediate, or Advanced proficiency requirements.
- **Your Certifications Still Count** Security+, CISSP, CySA+, CEH, GIAC, and CompTIA credentials remain valid — but how they qualify you is now determined by the DCWF work role you're filling, not a generic "Level II" label.
- **Compliance Deadlines Are Live** Cybersecurity element foundational qualifications were due February 15, 2025. IT, Cyber Effects, Intelligence (Cyber), and Cyber Enablers are due February 15, 2026. Cybersecurity resident qualifications follow February 15, 2027.

CONTENTS

01	The Shift from 8570 to 8140	Page 2
02	The DCWF Framework — Elements, Roles, Proficiency	Page 2
03	Qualification Pathways — Foundational vs. Resident	Page 3
04	Certifications That Still Drive Cleared Cyber Hiring	Page 3
05	Beginner's Roadmap into Cleared Cyber / IT	Page 4
06	Implementation Timeline & What It Means For You	Page 4

01 • THE SHIFT FROM 8570 TO 8140

For nearly two decades, DoD 8570.01-M defined cyber workforce qualifications through a simple grid: two categories (IAT for technical roles, IAM for management) and three levels each (I, II, III). A handful of commercial certifications mapped to each cell. It was straightforward — and increasingly outdated.

Why 8570 Was Retired

- Cyber roles grew far faster and more specialized than the IAT/IAM grid could capture (cloud, DevSecOps, threat hunting, AI/ML security, OT/ICS security).
- The framework rewarded credential collection over demonstrated capability — the certification didn't necessarily match what the person actually did on the job.
- It excluded large parts of the broader cyber workforce: cyber intelligence analysts, software developers building secure code, data scientists supporting cyber missions, program managers running cyber acquisitions.
- DoD needed a framework that could absorb new specialties as they emerged, instead of waiting for the next manual revision.

What DoDM 8140.03 Does Differently

- **Defines role-specific KSATs.** Each work role has documented Knowledge, Skills, Abilities, and Tasks (KSATs) describing what the person actually does.
- **Anchors to capability, not credentials.** Qualifications can be met through education, training, commercial certification, on-the-job experience, or military training — whichever pathway demonstrates the required KSATs.
- **Expands the scope.** Covers seven workforce elements, not just IT and IA. Includes cyber effects, intelligence, software engineering, data/AI, and enablers.
- **Builds in agility.** New work roles can be added to the DCWF as the threat and mission landscape evolves — without a full directive rewrite.

02 • THE DCWF FRAMEWORK

The DoD Cyber Workforce Framework (DCWF) is the standardized lexicon DoD uses to identify, track, and qualify every cyber-coded position across military, civilian, and contractor populations. Three concepts to know: workforce elements, work roles, and proficiency levels.

Seven Workforce Elements

- **Information Technology (IT)** System administration, network operations, infrastructure, enterprise IT.
- **Cybersecurity (CS)** Defensive operations, vulnerability management, incident response, security engineering, governance.
- **Cyber Effects (CE)** Offensive operations, cyber operations planning, cyberspace operations.
- **Intelligence (Cyberspace)** All-source cyber intelligence analysis, target development, exploitation analysis.
- **Data / Artificial Intelligence (Data/AI)** Data science, machine learning, AI engineering in cyber and mission contexts.
- **Software Engineering (SE)** Secure software design, development, testing, and DevSecOps in DoD environments.
- **Cyber Enablers** Acquisition, program management, training, legal, policy, and other roles supporting the cyber mission.

Work Roles & Proficiency

Across those seven elements, the DCWF currently defines roughly 70+ work roles. Each role lists its required KSATs at three proficiency levels:

- **BASIC** Entry-level competence. Performs work under supervision; foundational understanding of role-specific tasks.
- **INTERMEDIATE** Independent practitioner. Executes role responsibilities with minimal oversight; mentors junior team members.
- **ADVANCED** Senior expert. Leads complex initiatives, drives strategy for the work role, and develops the next generation of practitioners.

03 • QUALIFICATION PATHWAYS — FOUNDATIONAL vs. RESIDENT

DoDM 8140.03 separates qualifications into two complementary categories. Foundational qualifications establish your baseline capability to enter the role. Resident qualifications validate that you can demonstrate the role's KSATs in the actual job environment.

Foundational Qualifications

These prove you have the underlying knowledge and skills before stepping into the role. Acceptable options can include any of the following, as listed in the DoD 8140 Qualification Matrix at [cyber.mil](#):

- Approved commercial certifications (Security+, CISSP, CySA+, GIAC certs, vendor credentials, etc.)
- DoD-owned training courses (FedVTE, service-specific cyber schools, DCITA courses)
- Formal education (degrees from CAE-CD/CO/R designated institutions, NSA-sponsored programs)
- Military training and occupational specialty experience
- Demonstrated equivalent experience under documented review

Resident Qualifications

Foundational status gets you in the door; resident status confirms you can do the job once you're there. Resident qualifications are demonstrated on-the-job: completed training in the actual role, supervisor sign-off on KSAT execution, and continued professional development. Deadlines for resident qualifications follow foundational deadlines by approximately two years for each workforce element.

Source of Truth: The authoritative DoD 8140 Qualification Matrix lives at [cyber.mil](#). Components and contracts can impose stricter standards — always verify your specific role requirements with your hiring authority or FSO.

04 • CERTIFICATIONS THAT STILL DRIVE CLEARED CYBER HIRING

The certifications listed below remain widely accepted under DoDM 8140.03 — but they now qualify holders for specific DCWF work roles rather than generic IAM/IAT levels. The table below maps high-value certifications to the workforce elements where they carry the most weight.

WORKFORCE ELEMENT	HIGH-VALUE CERTIFICATIONS
Information Technology (IT)	CompTIA A+, Network+, Linux+ • Cisco CCNA / CCNP • Red Hat RHCSA • Microsoft Azure / AWS / GCP foundational certs
Cybersecurity (CS)	CompTIA Security+, CySA+, PenTest+, SecurityX (formerly CASP+) • ISC2 CISSP, SSCP, CCSP • ISACA CISM, CISA • GIAC GSEC, GCIH, GCIA, GCED • EC-Council CEH
Cyber Effects (CE)	OSCP, OSCE, OSEP • GIAC GPEN, GXPN, GREM • CEH Master / CPENT • CISSP (for leadership-track effects roles)
Intelligence (Cyberspace)	GIAC GCTI, GCFA, GREM, GNFA • CISSP • IC-specific training (per agency)
Data / AI	CompTIA Data+, DataX • AWS / Azure / Google ML & Data Engineering certs • Cloudera, Databricks credentials • Vendor-neutral AI/ML certifications (emerging)
Software Engineering (SE)	ISC2 CSSLP • GIAC GWEB, GSSP • AWS / Azure DevOps Engineer • Kubernetes (CKA / CKAD / CKS) • Scaled Agile (SAFe), CSM
Cyber Enablers	PMP, CAPM • ITIL 4 • ISACA CGEIT, CRISC • FAC-COR, DAWIA credentials • CMMC AB credentials (CCP, CCA)

05 • BEGINNER'S ROADMAP INTO CLEARED CYBER / IT

If you're entering the cleared cyber or IT workforce from scratch — transitioning out of the military, finishing school, or pivoting from a non-technical field — here's a no-nonsense progression that aligns with how the DoD 8140 framework actually hires.

Step 1 • Lay the Groundwork

- **CompTIA A+** Hardware, software, basic troubleshooting. The foundational IT credential.
- **CompTIA Network+** Networking fundamentals — essential for nearly any DoD cyber or IT role.
- **CompTIA Security+** The most widely required entry-level cyber credential for cleared work; maps to many DCWF Basic-level cybersecurity roles.

Step 2 • Pick a DCWF Work Role

Browse the DCWF work role catalog at cyber.mil. Pick one or two roles that match what you actually want to do day-to-day. Common starter roles: Systems Administration (IT), Network Operations (IT), Cyber Defense Analyst (CS), Vulnerability Assessment & Management (CS), All-Source Analyst (Intelligence).

Step 3 • Land an Entry-Level Cleared Role

- Help Desk / IT Support — ideal for clearance sponsorship while you build experience
- Junior Systems Administrator or Network Operations roles
- SOC Tier 1 / Cyber Defense Analyst — widely available, strong career progression
- DoD SkillBridge internships (last 180 days of military service — high-leverage path)

Step 4 • Stack Credentials and Experience

- CySA+ or GSEC for analyst-track progression
- PenTest+ or GPEN for offensive-track progression
- CISSP once you have 5+ years across two or more security domains (the single most impactful cert in cleared cyber)
- Cloud certifications (AWS / Azure) — increasingly required as DoD migrates to cloud

06 • IMPLEMENTATION TIMELINE & WHAT IT MEANS FOR YOU

DoDM 8140.03 sets phased compliance deadlines by workforce element. If you're currently in a coded DoD cyber role — or applying for one — these dates matter.

- **February 15, 2025 (Past)** Foundational qualifications deadline for the Cybersecurity workforce element.
- **February 15, 2026** Foundational qualifications deadline for IT, Cyber Effects, Intelligence (Cyber), and Cyber Enablers elements.
- **February 15, 2027** Resident qualifications deadline for the Cybersecurity workforce element.
- **Following years** Resident qualification deadlines for the remaining elements; Data/AI and Software Engineering elements continue rolling implementation.

*If your role is coded under the DCWF and you're not yet qualified, your component is required to bring you into compliance — typically through training, certification, or documented experience review. **Your IAM, ISSM, or FSO is the right starting point.***

ABOUT THIS GUIDE

Informational baseline only. The DoD 8140 Qualification Matrix at cyber.mil is the authoritative source — verify role-specific requirements with your IAM, ISSM, or FSO.

Sources: DoD CIO, cyber.mil, DoDM 8140.03.

QUESTIONS? REACH OUT.

Tier One Talent & Intel Recruiting

Veteran-Owned | Cleared | Federal Specialists

910.850.3055 • sgagliardi@tier1-talent.com • tier1-talent.com