GIAC offers a comprehensive certification portfolio, with twice as many the number of certifications offered by other providers, and integrates certification and education programs to meet DoD 8140 requirements fully. This approach ensures a practical understanding of skills crucial for the DoD, supported by double accreditation from the ANSI National Accreditation Board (ANAB) and Middle States.

### Directive Overview

Implemented in 2023, the DoD 8140 Directive establishes a comprehensive framework for developing a resilient, capable, and ready cyber workforce.

To address the expanding requirements, the DoD has standardized cybersecurity training, certifications, and education processes to ensure over 200,000 employees, service members, and contractors are adequately prepared. This unified approach enhances the capabilities of personnel across all levels.

### Certification Requirements

All individuals with access to critical DoD infrastructure must be certified. This includes:

- Service members
- DoD civilian employees
- Foreign nationals (those who work alongside the DoD)
- All DoD contractors (personnel who provide contracted services), including approved vendors for JEDI contract organizations (Google, Oracle, MSFT, and Amazon)

### Directive Compliance

Compliance with DoD Directive 8140 is mandatory for any DoD contractor or foreign national accessing sensitive information or networks. Adhering to these standards not only meets contractual obligations but also enhances the competitiveness of enterprises in securing government contracts, indicating a significant commitment to cybersecurity.

### Qualification and Maintenance Requirements

<table>
<thead>
<tr>
<th>Foundational Qualification:</th>
<th>Residential Qualification:</th>
<th>Annual Maintenance:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic to advanced proficiency; available through certifications (GIAC), training (SANS), and education (SANS EDU).</td>
<td>On-the-job qualifications must comprehensively address all relevant tasks and knowledge, skills, and abilities (KSAs) for the specified work role.</td>
<td>Maintenance of certification through Continuous Professional Education (CPE) or a minimum of 20 hours annually.</td>
</tr>
</tbody>
</table>

GIAC’s Role in DoD 8140 Compliance

GIAC offers a comprehensive certification portfolio, with twice as many the number of certifications offered by other providers, and integrates certification and education programs to meet DoD 8140 requirements fully. This approach ensures a practical understanding of skills crucial for the DoD, supported by double accreditation from the ANSI National Accreditation Board (ANAB) and Middle States.
GIAC Certifications and Corresponding Affiliate Training*

GIAC has the largest range of DoD-approved certifications, including:

### Cyber Defense
- GIAC Foundational Cybersecurity Technologies (GFAC T)
  SANS Foundations
- GIAC Information Security Fundamentals (GISF)
  SEC301: Intro to Cyber Security
- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Intrusion Analyst (GCIA)
  SEC503: Network Monitoring and Threat Detection In-Depth
- GIAC Continuous Monitoring Certification (GMON)
  SEC511: Continuous Monitoring & Security Operations
- GIAC Defensible Security Architect Certification (GDSA)
  SEC530: Defensible Security Architecture and Engineering Zero Trust

### Industrial Control Systems
- Global Industrial Cyber Security Professional Certification (GICSP)
  ICS410: ICS/SCADA Security Essentials
- GIAC Response and Industrial Defense (GRID)
  ICS515: ICS Visibility, Detection, & Response

### Educational Opportunities
- SANS Technology Institute offers cybersecurity degrees and certificate programs.

*Additional certification options are continuously being added to the DoD8140 Directive.

### Compliance Timeline

**DoD Cybersecurity Workforce**
- Foundational qualifications due by: **February 15, 2025**
- Residential qualifications due by: **February 15, 2026**

**Other DoD Cyberspace Workforce Elements**
- Foundational qualifications due by: **February 15, 2026**
- Residential qualifications due by: **February 15, 2027**

**Digital Forensics & Incident Response**
- GIAC Certified Forensic Examiner (GCFE)
  FOR500: Windows Forensic Analysis
- GIAC Certified Forensics Analyst (GCFA)
  FOR508: Advanced Incident Response, Threat Hunting & Digital Forensics
- GIAC Cyber Threat Intelligence (GCTI)
  FOR578 Cyber Threat Intelligence
- GIAC Reverse Engineering Malware Certification (GREM)
  FOR610: Reverse-Engineering Malware

**Offensive Operations**
- GIAC Incident Handling Certification (GCIH)
  SEV504: Hacker Tools, Techniques, and Incident Handling
- GIAC Penetration Tester Certification (GPEN)
  SEC560 Enterprise Pen Testing

**Cloud Security**
- GIAC Cloud Security Essentials Certification (GCLD)
  SEC488: Cloud Security Essentials
- GIAC Cloud Security Automation (GCSA)
  SEC540: Cloud Security & DevSecOps Automation

**Cybersecurity Leadership**
- GIAC Security Leadership (GSLC)
  LDR512: Security Leadership Essentials for Managers
- GIAC Strategic Planning, Policy, and Leadership (GSTRT)
  LDR514: Security Strategic Planning, Policy, and Leadership

"Attackers are always evolving, and having a GIAC certification prepares you to evolve with them. It allows you to implement the appropriate methods and best practices in your company while understanding it’s a continuous fight."

- Jason Sevilla | GCIH, GMON, GSEC

Explore more at GIAC
www.giac.org/workforce-development/dodd-8140/