1. Introductions – SANS GIAC Team
2. Goal: 2017 Executive Order
3. SANS GIAC NICE Workforce Framework (NCWF) Mapping Overview
4. Workforce Development Discussion
5. Q&A
By the authority vested in me as President by the Constitution and the laws of the United States of America, and to protect American innovation and values, it is hereby ordered as follows:

Section 1. Cybersecurity of Federal Networks.

(a) Policy. The executive branch operates its information technology (IT) on behalf of the American people. Its IT and data should be secured responsibly using all United States Government capabilities. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise.

(b) Findings.

(i) Cybersecurity risk management comprises the full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

(ii) The executive branch has for too long accepted antiquated and difficult-to-defend IT.
May 11, 2017: President Trump issued an Executive Order to strengthen federal networks and critical infrastructure cybersecurity

- President will hold agency heads accountable for managing cybersecurity risk
- Agency heads shall use the NIST Framework to manage their agency’s cybersecurity risk framework
- U.S. seeks to support the growth and sustainment of a workforce that is skilled in cybersecurity and related fields
Broad Organization of the NICE Framework


GIAC Certifications 2017, Version 1.3
• Mapped SANS training courses and GIAC certifications to the NCWF

• One slide/card per NICE job role
  • Everything you need to know about that job role, specialty area, and mapped SANS/GIAC offerings in one page

• Includes SANS Course, GIAC Certification, and Proficiency Levels

• High road approach
  • Integrity in mapping
  • IOW – Not trying to fill in boxes where it doesn’t make sense
About Proficiency Levels

- **Basic** - Training maps to many knowledge statements, simpler skills, and tasks that are pre-requisites to an employee being effective in this job role.

- **Intermediate** - Training maps to many mid-level knowledge, skills, abilities and tasks. Employee can be reasonably effective in this job role after receiving training.

- **Advanced** - Maps to higher level knowledge, skills, abilities, and tasks. Employee should be very effective in this functional area after receiving training. However, some lower level, pre-requisite KSAs may not be covered by these courses.

- **Expert** - Maps to few very specific KSAs or tasks in a highly focused area. This training assumes someone is already well trained and effective in this job role overall. It focuses on expertise in a very specific, narrow area.
Best Fit for Most People

Other mapped offerings, may be more basic, advanced, or specialized than the majority will need.

Other Mapped SANS Training and GIAC Certifications:
SEC401: Security Essentials Bootcamp
GSEC: GIAC Security Essentials
**Specialty Area: Digital Forensics (FOR)**
Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

**Work Role: Cyber Defense Forensics Analyst (IN-FOR-002)**
Analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

<table>
<thead>
<tr>
<th>SANS Training Course</th>
<th>GIAC Certification</th>
<th>NICE Proficiency Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOR500: Windows Forensics Analysis</td>
<td>GCFE: GIAC Certified Forensic Examiner</td>
<td>3: Advanced</td>
</tr>
<tr>
<td>FOR572: Advanced Network Forensics and Analysis</td>
<td>GNFA: GIAC Network Forensic Analyst</td>
<td>3: Advanced</td>
</tr>
</tbody>
</table>

**Other Mapped SANS Training and GIAC Certifications:**
- FOR585: Advanced Smartphone Forensics / GASF: GIAC Advanced Smartphone Forensics
- FOR518: Mac Forensic Analysis
- FOR526: Memory Forensics In-Depth
Specialty Area: Vulnerability Assessment and Management (VAM)
Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.

Work Role: Vulnerability Assessment Analyst (PR-VAM-001)
Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

<table>
<thead>
<tr>
<th>SANS Training Course</th>
<th>GIAC Certification</th>
<th>NICE Proficiency Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC560: Network Penetration Testing and Ethical Hacking</td>
<td>GPEN: GIAC Certified Penetration Tester</td>
<td>3: Advanced</td>
</tr>
<tr>
<td>SEC660: Advanced Penetration Testing, Exploit Writing, and Ethical Hacking</td>
<td>GXPN: GIAC Exploit Researcher and Advanced Penetration Tester</td>
<td>4: Expert</td>
</tr>
<tr>
<td>SEC642: Advanced Web App Penetration Testing, Ethical Hacking, and Exploitation Techniques</td>
<td>N/A</td>
<td>4: Expert</td>
</tr>
</tbody>
</table>
Specialty Area: Vulnerability Assessment and Management (VAM)
Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.

Work Role: Vulnerability Assessment Analyst (PR-VAM-001)
Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Other Mapped SANS Training and GIAC Certifications:
SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling / GCIH: GIAC Certified Incident Handler
AUD507: Auditing & Monitoring Networks, Perimeters & Systems / GSNA: GIAC Systems and Network Auditor
ICS515: ICS Active Defense and Incident Response / GRID: GIAC Response and Industrial Defense
SEC617: Wireless Penetration Testing and Ethical Hacking / GAWN: GIAC Assessing Wireless Networks
SEC561: Immersive Hands-on Hacking Techniques
SEC562: CyberCity Hands-on Kinetic Cyber Range Exercise
SEC760: Advanced Exploit Development for Penetration Testers
• What is your agency doing to meet the EO requirements?
• OSD Update
• Other examples?
SANS Workforce Development Capabilities

**How Our Capabilities Are Helping Clients**

- **Recruit**
  - Assessing Aptitude
  - CyberStart
  - Academies
- **Develop**
  - Assessing Skills
  - *SANS Training (mapped to NCWF)*
  - *GIAC Certifications (mapped to NCWF)*
  - Roadmaps
- **Retain**
  - Cyber Ranges and Exercises
  - Master’s Degree/Certificate Programs
SANS Federal Team

- Daryl Gilbertson (US Army, USAF): DGilbertson@sans.org
- Matt Beaghley (US Navy, USCG, USMC, DOE): mbeaghley@sans.org
- Mike Forostiak (Federal Civilian Agencies): MForostiak@sans.org
- Jim Yacone (Intel/Law Enforcement Community): JYacone@sans.org
- John Nix: JNix@sans.org

Download this presentation at https://www.giac.org/certifications/niceframework
What is SANS?

- **Global, trusted** leader in Information Security training, certification, education, and research
  - 30,000+ individuals trained annually
  - 70 courses across multiple curriculums
- Deep, **comprehensive** offering
- **Expert** instructors (teachers) → Exceptional course content
- Focus: **Applied Skills**
- Validated **Quality**
- Proven, **flexible** learning formats (live in-classroom or online)
SANS Suite of offerings

SANS NetWars
Testing hands-on technical skills in a safe environment so security professionals are prepared when a real incident occurs.

SANS Training
Hands-on security training for professionals just starting in security up to seasoned professionals. Training courses are delivered at live events and online.

SANS CyberTalent
Assess the skills and aptitude of security professionals so you can feel confident in your hiring decisions.

SANS Security Awareness
Everything your organization needs for an effective security awareness program.

SANS Technology Institute
A regionally accredited postgraduate institution focused solely on information security education for working professionals.

GIAC Certification
Validate the technical skills and knowledge of your security professionals.