Workcred—*The Value of Credentialing to Cybersecurity*

Clif Triplett Senior Cyber & Information Technology Advisor
Office of Personnel Management

October 11, 2016
During the first five months of FY 2015 (10/2014 – 2/2015), the number of Cybersecurity separations were at least twice the number of Cybersecurity accessions, and in January, there were almost four times as many separations. Sustained separation ratios like those could cripple the Cybersecurity workforce.
National Cybersecurity Workforce Framework

7 Categories of the Workforce Framework

*graphic from NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES
National Cybersecurity Workforce Framework and OPM Codes

**Cybersecurity Work Categories and Specialty Areas**

- The OPM Data Element codes and the NICE Framework re-define cybersecurity work using 31 Specialty Areas (SA), organized into distinct work Categories.
- Organizations can use these data to identify, build, and customize cybersecurity roles based on mission.

---

**Collect and Operate**

- [30] Program/Project Management
- [31] Cyber Operations Planning
- [32] Exploitation Analysis
- [33] Cyber Operations
- [34] Digital Forensics
- [35] Forensic Analysis

**Investigate**

- [21] Cyber Threat Analysis
- [22] Cyber Operations Planning
- [23] Investigation
- [24] Domain Awareness
- [25] Data Analysis

**Analyze**

- [10] Analysis
- [11] All Source Intelligence
- [12] Cyber Threat Analysis
- [13] Targets
- [14] Cyber Threat Management

**Collect and Operate**

- [15] Cyber Threat Analysis
- [16] Cyber Threat Mitigation
- [17] Cyber Threat Management
- [18] Cyber Threat Response
- [19] Cyber Threat Assessment

**Protect and Defend**

- [50] Computer Network Defense (CND)
- [51] Vulnerability Assessment and Management
- [52] Incident Response
- [53] Information Security Operations
- [54] Information Assurance (IA)

**Operate and Maintain**

- [40] System Administration
- [41] Network Services
- [42] Data Administration
- [43] Knowledge Management
- [44] Information Assurance (IA)

**Oversight and Development**

- [70] Legal Advice and Advocacy
- [71] Education and Training
- [72] Systems Security Operations
- [73] Systems Development
- [74] Technology Research and Development

**Securely Provision**

- [60] Systems Requirement Planning
- [61] Systems Development
- [62] Software Assurance and Security Engineering
- [63] Customer Service and Technical Support
- [64] Technology Research and Development

---

[00] Not Applicable

[90] Supervision, Management, and Leadership

[80] Program/Project Management

[70] Knowledge Management

[60] Information Assurance (IA)
Most of the Cybersecurity workforce functions being performed in the Federal Government are in the “Operate and Maintain” work category. This includes the Cybersecurity work being done by contractors, as well as the Federal Cybersecurity workforce. Fifty percent of the Federal Cybersecurity workforce, 53% of Federal Cybersecurity accessions, and 34% of all estimated contractor support needed is in the Operate and Maintain category.
Top 5 Projected Cybersecurity NICE Work Roles

- It is projected that between 2016-2019 up to 10,000 cyber professionals will be needed to support the anticipated demand.

- Customer Service and Technical Support (41);
- System Administration (45);
- Network Services (44);
- Information Systems Security Operations (72); and
- Operate and Maintain (40).
The Federal Cybersecurity workforce is spread out across and outside of the United States, but is most heavily concentrated on the **East Coast (Virginia, Maryland, and the District of Columbia) and in California and Texas.** The Cybersecurity workforce is well represented by Veterans and Federal agencies continue their commitment to hiring from this pool of talent. In FY 2015, **62%** of new hires and transfer ins made to the Cybersecurity workforce were **Veterans.**
Cybersecurity Human Capital Strategy (at a glance)

Make civilian Federal service the destination of choice for Cybersecurity professionals throughout multi-sector careers

Data Analytics
Increase cybersecurity workforce data accuracy and planning capability to effectively conduct workforce planning.

Talent Pipeline
Work with educational institutions on a cyber curriculum from K-12 through university to significantly increase capacity for government and beyond.

Recruit & Hire
Engage in government-wide and agency-specific efforts to conduct outreach and recruitment for cybersecurity talent.

Talent Development & Retention
Promote retention through uniform, high-quality trainings, certifications, badging, and developmental opportunities across the Federal cybersecurity workforce.
Purpose: Establish an enterprise-wide approach to retention and development to support the continued enhancement of the cybersecurity workforce and its infrastructure.

Outcome: Create a network of cybersecurity professionals to facilitate knowledge sharing, identify potential cybersecurity professionals inside the Federal workforce, and promote long-term professional development through informal and formal channels to improve retention efforts and incentivize greater workforce capabilities.
The Federal Government Cybersecurity Professional Credentialing Framework will promote awareness, recognition, and achievement for the cybersecurity professional, and promote the Federal Government as an employer of choice. Moreover, the government wide framework would provide recognition and reciprocity across agencies. This unique program, that reflects mastery and prestige at elite levels, will contribute to attracting and retaining top talent and foster duty, mission, teamwork, comradery, and professional pride in service to the nation. Modeled after the highly successful examples in the US military, the credentialing of Federal cybersecurity professionals will recognize the most highly qualified subject matter experts in the field with competencies that address the critical needs of the Federal Government, as well as desired expertise in private industry.
What are the possibilities a credentialing program might enable?

• Recruit
  – Aspirational achievement opportunities
  – Financial incentives
  – Unique career possibilities

• Retain
  – Pride
  – Compensation possibilities
  – Career goals and pathways

• Skills Recognition Reciprocity

• Surge Force
The Model Being Considered –
2 Major Dimensions

• Employee Skill Evolution
  – Apprentice
  – Journeyperson
  – Expert

• Training Program Levels
  – Foundation (Level 1)
  – Role Based/ Journeyperson (Level 2)
  – Expert
  – Elite

*Focus for Credentialing*
Level 3 (Expert) Training Criteria Concept

- Concentrated practical experience (real world experience) or Simulated experience
- Course work
- Ability and willingness to complete exceptionally challenging training regimen
- 2+ year commitment to service
- Peer reviews as part of criteria to earn badge
- Ability to lead and instruct small teams
- Credential level
- Stipend offered for approved items
- Federal only credentialing

*Working Concept Only / Deliberative / Pre-Decisional*
Level 3 (Expert) Training Requirements for Participation

- Nomination (could be from governance board / competition/simulator score)
- Personality Attribute Testing
- Competency testing
- Extraordinary job performance
- Re-qualify

Working Concept Only / Deliberative / Pre-Decisional
Level 4 (Elite) Training Criteria Concept

• Best of the Best generally selected from those with Prestige Badges
• Three years of superior performance and continuous training or mission experience.
• Selected from superior active Prestige Badge corps
• Credential level
• Stipend offered for approved items
• Federal only credentialing

Working Concept Only / Deliberative / Pre-Decisional
Level 4 (Elite) Training Requirements for Participation

- Selected from top performing active expert badge holders
- Exceptional performance demonstrated and validated by the Elite organization
- Re-qualify

Working Concept Only / Deliberative / Pre-Decisional
# Illustration of the Concept

<table>
<thead>
<tr>
<th>Levels</th>
<th>Military Recognition</th>
<th>Cyber Illustrations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elite (Level 4)</td>
<td>Seal Team Six / Delta</td>
<td>Cyber Force 1*</td>
</tr>
<tr>
<td>Expert (Level 3)</td>
<td>Navy Seal / Army Ranger</td>
<td>Cyber Investigator*</td>
</tr>
<tr>
<td>Journeyperson (Level 2)</td>
<td>Airborne / Air Assault</td>
<td>Cyber Defender*</td>
</tr>
<tr>
<td>Apprentice (Level 1)</td>
<td>Marksman</td>
<td>Cyber Warrior*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CISSP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft Certified Solutions Expert (MCSE)</td>
</tr>
</tbody>
</table>

* Illustrative Only
Cybersecurity Credentialing Initiative Summary

- Program targeted to be recognized across the Federal Workspace providing reciprocity skills attainment and credentialing across agencies
- Leverages the NICE framework from NIST
- Provides value in managing and motivating the cyber workforce
- Badging and Credentialing initiative targeted for launch in 2017