NICE Framework Competencies
Moving from Concept to Implementation

Tuesday, March 23, 2021 & Thursday, March 25, 2021

CAE in Cybersecurity Community Virtual Event
https://www.caecommunity.org
Workforce Framework for Cybersecurity (NICE Framework) Competencies Workshop

Opening and Welcome
Rodney Petersen, Director, NICE

nist.gov/nice
Credentials and Competencies in NICE Strategic Plan

• **Promote the Discovery of Cybersecurity Careers and Multiple Pathways**
  – Increase understanding of multiple learning pathways and credentials that lead to careers that are identified in the Workforce Framework for Cybersecurity (NICE Framework)

• **Transform Learning to Build and Sustain a Diverse and Skilled Workforce**
  – Improve the quality and availability of credentials (e.g., diplomas, degrees, certificates, certifications, badges) that validate competencies
  – Facilitate increased use of performance-based assessments to measure competencies and the capability to perform NICE Framework tasks
  – Encourage the use of Learning and Employment Records to document and communicate skills between learners, employers, and education and training providers

• **Modernize the Talent Management Process to Address Cybersecurity Skills Gaps**
  – Align qualification requirements according to proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework
Credentials and Competencies in Recent NICE Webinars

- February 2021 – Advancing Skills-Based Education and Hiring Through the Open Skills Network
- January 2021 – The Credentialing Economy and What It Means for Cybersecurity Skills
- December 2020 – Competencies – The Next Frontier for Closing the Cybersecurity Skills Gap
- October 2020 – Introducing Learning and Employment Records – Addressing the Cybersecurity Talent Gap at Scale

https://www.nist.gov/itl/applied-cybersecurity/nice/events/webinars
Why A Community Approach to Competencies Is Important

• Common taxonomy and lexicon as an extension of the NICE Framework
• Shared methods for competency development for learners
• Effective techniques for learners to evidence competencies
• Usable approaches for small- and medium-sized employers
• Close the gap between employer and credential provider assessments

Moving from Concept to Implementation
Workshop Overview

Karen A. Wetzel
Manager of the NICE Framework, NICE
### Day 1: Understanding Use Cases

- Opening & Welcome
- Workshop Overview
- Competencies & the NICE Framework
  - Presentation & Discussion
- Coffee Break
- Breakouts: Understanding Competency Use Cases
  - Introduction
  - Breakout Part 1
  - Rejoin
  - Breakout Part 2
- Snack Break
- Sharing Out: Coming to Consensus
- Closing Session: Recap

### Day 2: Focus on Proficiencies & Assessment

- Opening Session
- Proficiencies & Assessment (Guest Speakers)
- Coffee Break
- Breakouts: Putting Competencies into Practice
  - Introduction
  - Breakout Part 1
  - Rejoin
  - Breakout Part 2
- Snack Break
- Sharing Out: Moving Forward
- Closing Session: Next Steps
Karen Bane, Facilitator
Workshop Goals

**Defined use cases** that show how NICE Framework Competencies can be used (and identify what work is outstanding).

The role of **assessment and proficiencies** and ideas on how to shift from concept to practice.

Clear understanding of the greatest **benefits to and challenges in** implementation.

**Next steps** that NICE should take, including how ideas raised at this workshop should be brought forward.
Housekeeping & Ground Rules

→ Slides will be shared following the event
→ Recording of main sessions for internal review only
→ Mute when not speaking
→ A workshop report will follow

→ Be present
→ Share and listen
→ Stay on track
→ Think big
Why Competencies?

Karen A. Wetzel
Manager of the NICE Framework, NICE
karen.wetzel@nist.gov
Why Competencies?

- Evolving Recruiting Practices
  - Shift from [only] degree-based to [also] competency-based hiring
  - Broader applicant pool
  - Qualified candidates for emerging technologies

- Assessment-based hiring and promotion
- Identify current gaps and anticipate future needs
- Align education and training to organizational goals
What Competencies Offer

- A high-level perspective on cybersecurity work
- A flexible and responsive approach to shifting needs
- A way for organizations to succinctly communicate and effectively organize cybersecurity needs to provide a streamlined view of the workforce

Improved Outcomes
Bridge Stakeholders

NICE Framework

define

COMPETENCIES that learners possess, acquire, develop

identify

assess

Employers

Education, Training Providers, Employers
A clearly articulated, observable framework for what success looks like.

“Why Competencies Are the Future of HR” (HR Magazine/SHRM: April 2017)
A Consistent Model...

- Enables the establishment of regular processes – from hiring to training and assessment – across an organization.
- Shares clear information about cybersecurity workforce needs to help students, job-seekers, and workers develop, demonstrate, or improve their competencies.
- Provides direct information about what a workforce needs to know, helping in the development of certificates, badging, and other verification techniques to consistently describe learner capabilities.
NICE Framework: Building Blocks

Describes the Work

Describes the Learner
NICE Framework Competencies

Competency:
A mechanism for organizations to assess learners.

Competencies are:
• Defined via an employer-driven approach
• Learner-focused
• Observable and measurable

Consist of:
• Competency title
• Competency description
• Associated TKS statements

Call for Comments:
March 17 – May 3
Draft NISTIR 8355
NICE Framework Competencies:
Assessing Learners for Cybersecurity Work
https://csrc.nist.gov/publications/detail/nistir/8355/draft
How can I use Competencies?

**Employers**
- Track workforce capabilities
- Position descriptions
- Assess learner capabilities
- Develop teams

**Education & Training Providers**
- Develop a learning program
- Focus teaching on associated K&S
- Test whether learners have achieved capabilities

**Learners**
- Learn about a defined area of expertise
- Understand an organization’s workforce needs
- Self-assessment
Discussion

- How does this fit with your concept of competencies?
- What seems promising to you about competencies?
- What questions do you still have?
Understanding Competency Use Cases: Introduction to Break-out Sessions

Karen Bane, Facilitator
March 23 Closing Session

Thursday, March 25
Focus on Proficiencies & Assessment

Lisa Dorr
Senior Talent Management Strategist, DHS

Max Shuftan
Director, CyberTalent Programs
SANS Institute

THANK YOU!
NICE Framework Competencies
Moving from Concept to Implementation

DAY 2
Thursday, March 25, 2021

CAE in Cybersecurity Community Virtual Event
https://www.caecommunity.org
Opening & Welcome

Karen A. Wetzel
Manager of the NICE Framework, NICE
Understanding Proficiencies & Assessment

Marian Merritt
Deputy Director and Lead for Industry Engagement, NICE
Today’s Speakers

**Lisa Dorr**  
Senior Talent Management Strategist, Cybersecurity and Intelligence Talent Experience (CITE) Division  
Office of the Chief Human Capital Officer  
Department of Homeland Security

**Max Shuftan**  
Director, CyberTalent Programs  
SANS Institute
Lisa Dorr, Senior Talent Solutions Manager

Department of Homeland Security
Office of the Chief Human Capital Officer

- Cybersecurity and Intelligence Talent Experience (CITE) Division
- Cybersecurity Talent Management System (CTMS) Innovations Team
- Senior Talent Solutions Manager for Strategic Analysis & Change Management and Talent Engagement & Development
Cybersecurity Mission Objectives Drive Workforce Needs

Performance Objectives

- Risk Identification
- Vulnerability Reduction
- Threat Reduction
- Consequence Mitigation
- Enabled Cybersecurity Outcomes

Cybersecurity Mission
Mission-Driven Qualifications

Education and Experience

Preferred Degree Types and Certifications

Capabilities

Technical Competencies

Behavioral Indicators/Benchmarks and Proficiency Levels
Key Terms

- **Occupation** - A job family with vertical progression through similar functional competencies at different levels of proficiencies

- **Role** - Homogeneous grouping of individual positions based on similarity in activities performed, competencies required, and goals or outcomes accomplished. This is a responsibility that a person will/might perform for a period in time during his/her career

- **Position** – Combines specific occupation, level, role work responsibilities, and activities performed by one person

- **Task** – Describes an activity to be performed by an individual within a particular role (e.g., creates user accounts)

**Example:**
- **My Occupation** → IT 2210 InfoSec Professional (Federal Employee) Cybersecurity Professional (Private Sector)
- **My Role(s)** → Cybersecurity Analyst (Fed/Private Sector)
- **My Position** → GS-12 Cybersecurity Analyst (Federal Employee) Associate Cybersecurity Analyst (Private Sector)
- **My Level** → GS 12 (Federal Employee) Associate (Private Sector)
**Setting Targets and Measuring Proficiencies of Competencies**

<table>
<thead>
<tr>
<th>Competency Definition</th>
<th>Competency Definition: This definition is like a mission statement for the Competency. It is a broad statement that sets the scope for the for the Competency.</th>
</tr>
</thead>
</table>

**Example Tasks Identified as Part of Competency:**
These tasks are included to give context around the competency. This is not meant to be an exhaustive list, but rather a few examples that came up during the conversation with the subject matter experts.

**Behavioral Indicators**
(Describes how the competency manifests itself in observable on the job behavior)

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Foundational Knowledge • I do not have the sufficient knowledge or skills necessary in this area for use in simple or routine work situations. Any awareness, knowledge, or understanding I do have would be considered common, similar to that of a layperson. Considered &quot;no proficiency&quot; for purposes of accomplishing work.</td>
</tr>
<tr>
<td>1</td>
<td>Basic • I have the basic knowledge and skills necessary in this area for use and application in simple work situations with specific instructions and/or guidance.</td>
</tr>
<tr>
<td>2</td>
<td>Intermediate • I have the intermediate knowledge and skills necessary in this area for independent use and application in straightforward, routine work situations with limited need for direction.</td>
</tr>
<tr>
<td>3</td>
<td>Advanced • I have the advanced knowledge and skills necessary in this area for independent use and application in complex or novel work situations.</td>
</tr>
<tr>
<td>4</td>
<td>Expert • I have the expert knowledge and skills necessary in this area for independent use and application in highly complex, difficult, or ambiguous work situations, or I am an acknowledged authority, advisor, or key resource in this area</td>
</tr>
</tbody>
</table>

**Criticality**
Importance
Identifies the competencies required on day 1 of the job versus those that can be learned over time

<table>
<thead>
<tr>
<th>Importance</th>
<th>Required at Entry</th>
<th>Criticality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = Not at all Important</td>
<td>1 = Not Required</td>
<td>An evaluation of Importance and Required at Entry ratings to determine which competencies could be used to make personnel decisions</td>
</tr>
<tr>
<td>5 = Extremely Important</td>
<td>3 = Definitely Required</td>
<td></td>
</tr>
</tbody>
</table>

**Proficiency Targets**
Establishes the significance of the competency to successful performance in the occupation

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Identifies the proficiency at which a person in a specific career level should be performing. Aligns with the Behavioral Indicator descriptions above (Career levels will differ by occupation)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Sample tasks to help illustrate the competency.**

**Criticality is determined by combining the ratings of competency importance plus required upon entry.**

---

**Behavioral indicators (BI) are identified across four proficiency levels.**

---

**Proficiency Targets are the degree in which an individual would be expected to be proficient based on their career level within the role.**
## Cybersecurity Analyst Competencies

<table>
<thead>
<tr>
<th>Illustrative Example</th>
<th>Security Monitoring and Event Analysis</th>
<th>Digital Forensics</th>
<th>Exploitation Analysis</th>
<th>Incident Response</th>
<th>Investigation</th>
<th>Cyber Threat Analysis</th>
<th>Cyber Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proficiency Level Targets for Cybersecurity Analyst Career Levels</td>
<td>Entry/Tier 1 (GS 7 GS 9)</td>
<td>Tier 1 (GS 11 GS 12)</td>
<td>Tier 2 GS 13</td>
<td>Lead GS 14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Illustrative Example

### Shared Competencies Among GS-12/ Cybersecurity Specialists, Performing In Different Work Roles

<table>
<thead>
<tr>
<th>Competency</th>
<th>Cybersecurity Analyst</th>
<th>Penetration Tester</th>
<th>Security Architect</th>
<th>Policy Lead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Network Defense Analysis</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Security Monitoring and Event Analysis</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Digital Forensics</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Exploitation Analysis</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Cyber Operations</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

### Proficiency Level Targets for Cybersecurity Roles
Proficiency Targets are Foundational to the Talent Management Lifecycle

Proficiency in Practice

- Position Descriptions
- Hiring Assessments
- Talent Development, Retention, and Succession Planning
- Performance Management and Recognition
- Behavioral-Based Interview Questions
# Practices of Yesterday & Today

<table>
<thead>
<tr>
<th>Traditional Practices</th>
<th>Today’s Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning for employment for life</td>
<td>Planning for today’s gig</td>
</tr>
<tr>
<td>Career ladders progressing upward in a linear fashion</td>
<td>Multi-Track career paths with lattices progressing up, down, sideways, and/or in and out</td>
</tr>
<tr>
<td>Job announcements, branding, outreach, and candidate vetting</td>
<td>Apps, Buzz Feeds, and “apply now” buttons</td>
</tr>
<tr>
<td>Static training classes completed in an ad hoc, reactionary fashion</td>
<td>Formal mentoring, shadowing, and rotation programs and dedicated attention from senior leaders to “show the ropes”</td>
</tr>
<tr>
<td>Off-the-shelf career interest inventories</td>
<td>Personalized skills and capability-based benchmarking assessments</td>
</tr>
<tr>
<td>Success measured by upward progress and increase in salary</td>
<td>Success measured by perpetual growth in knowledge &amp; experience</td>
</tr>
<tr>
<td>In the classroom, formal learning and development offered periodically</td>
<td>On-the-job learning and experience-building offered continuously and supported by relationships and networks</td>
</tr>
<tr>
<td>Next-level job definition</td>
<td>Full career mapping plans for job roles and/or capability areas</td>
</tr>
<tr>
<td>No integration with succession management, performance management, or L&amp;D</td>
<td>Full integration with succession management, performance management, L&amp;D and other talent processes</td>
</tr>
<tr>
<td>No, or very limited, focus on building personal brand</td>
<td>All about building personal brand</td>
</tr>
<tr>
<td>Doing what you’ve been told to do and know how to do</td>
<td>Doing what you are good at and being given the opportunity to learn how to do it better</td>
</tr>
<tr>
<td>Limited career information available</td>
<td>All career information is widely available and broadcast to all employees across the enterprise</td>
</tr>
<tr>
<td>No focus on creating large, diverse talent pools</td>
<td>Focused on creating large, diverse talent pools</td>
</tr>
</tbody>
</table>

*Source: Brandon Hall Group*
Thank you!
Promising Practices in Cyber Talent Assessments

Max Shuftan
Director, CyberTalent Programs
SANS Institute
Common Problems

Retraining
Which individuals who have not worked in IT or security are most likely to excel in advanced cybersecurity training and become top performers?

Upskilling
How advanced are the competencies of current cybersecurity employees and what do they need to learn to move to higher levels of performance?

Recruiting
Which candidates have the technical, hands-on skills or knowledge needed to perform hard-to-fill mission critical roles?

Talent of the future
Which of these students can be a cyber star? Who has curiosity, tenacity, problem solving skills and loves learning new things?
Retraining

Which of these individuals who have not worked in IT or security are most likely to excel in advanced cybersecurity training and become top performers?

- CYBERCOM request to Army, Airforce and Navy/Marines for 3,300 technical cyber experts (each): “I don’t have 30!”

- How do we find the active-duty service members who can become top performers in cybersecurity?

- UAE being attacked by Iran: “How do we find citizens who can be trained and become our “cyber falcons?”

- United Kingdom and Canada seeking retraining opportunities for citizens
## Evolution of assessment for retraining programs

<table>
<thead>
<tr>
<th>Phase</th>
<th>Find any available candidates</th>
<th>Grueling 26-week cyber boot camp on technology, networking, Linux, Windows, etc.</th>
<th>High 22-26% failure rate</th>
<th>Train in cybersecurity for incident response, red teams, defense, and more</th>
<th>Only about 3% were top performers and 20-30% did well</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Find candidates with cyber aptitude</td>
<td>Grueling cyber boot camp training</td>
<td>Lower failure rate</td>
<td>Train in cybersecurity for incident response, red teams, defense, and more</td>
<td>More (the hobbyists) were top performers and more also did well</td>
</tr>
</tbody>
</table>

Only about 3% were top performers and 20-30% did well.
Phase 2: Aptitude assessment

“Cyber falcons are the go-to people on every problem we have to solve”
Evolution of assessment for retraining programs

**Phase 1**
Find any available candidates
- Grueling 26-week cyber boot camp on technology, networking, Linux, Windows, etc.
- High 22-26% failure rate
- Train in cybersecurity for incident response, red teams, defense, and more
- Only about 3% were top performers and 20-30% did well

**Phase 2**
Find candidates with cyber aptitude
- Grueling cyber boot camp training
- Lower failure rate
- Train in cybersecurity for incident response, red teams, defense, and more
- More (the hobbyists) were top performers and more also did well

**Phase 3**
Find candidates with tenacity, quick learning, and cyber aptitude
- Accelerated training program for performance-based assessments
- Minimal failure; incredibly high success rates
- Train in cybersecurity for incident response, red teams, defense, and more
- Many more top performers and most do well
Upskilling

How advanced are the skills of our current cybersecurity employees and what do they need to learn to move to higher levels of performance?

• Promising practices:

• Look for skills gaps?
  • Lab-based assessments?
  • Knowledge within a specialty area?

• Levels of competency determined by certification exams?
Recruiting

Which candidates have the technical, hands-on skills or knowledge needed to perform hard-to-fill mission critical roles?

• Promising practices:

• Certifications as a standard?

• Knowledge-based tests

• Hands-on skill assessments, lab-based testing

• Using tournaments and competitions to evaluate candidates
Which of these students can be a cyber star? Who has curiosity, tenacity, problem solving skills and loves learning new things?

• Waiting too long to identify cyber talent
• Start in middle and/or high school to broaden pipeline
• HMG Cyber Discovery Program in the UK
### HMG Cyber Discovery

Program that assesses, develops and motivates young talent – rapidly at national scale:

<table>
<thead>
<tr>
<th></th>
<th>4-year goal</th>
<th>First year</th>
<th>End of 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Students assessed in Game</td>
<td>20,000</td>
<td>23,000</td>
<td>200,000</td>
</tr>
<tr>
<td>Students taking foundational training</td>
<td>6,000</td>
<td>9,000</td>
<td>38,000</td>
</tr>
<tr>
<td>Elite scorers – cyber stars</td>
<td>600</td>
<td>700</td>
<td>4,500</td>
</tr>
</tbody>
</table>

**Categories and Topics**

- Computer Hardware (OS)
- Linux and Windows
- Networking
- Programming
- Common Attacks & Security
- Ethical Hacking (Kali, Google, etc.)

**Modules**

- 6
- 7
- 6
- 6
- 10
- 11
Common Problems

**Retraining**
Which individuals who have not worked in IT or security are most likely to excel in advanced cybersecurity training and become top performers?

**Upskilling**
How advanced are the competencies of current cybersecurity employees and what do they need to learn to move to higher levels of performance?

**Recruiting**
Which candidates have the technical, hands-on skills or knowledge needed to perform hard-to-fill mission critical roles?

**Talent of the future**
Which of these students can be a cyber star? Who has curiosity, tenacity, problem solving skills and loves learning new things?
Questions?

Contact:
Max Shuftan
mshuftan@sans.org
Proficiencies & Assessment Discussion
Putting NICE Framework Competencies into Practice
Introduction to Break-out Sessions

Karen Bane, Facilitator
Closing Session

Recap & Next Steps
How to Engage

Visit the NICE Framework Resource Center
www.NIST.gov/NICE/Framework

Contribute your Success Story idea and
Comment on Competencies
niceframework@nist.gov

Join the NICE Framework Users Group to
discuss and learn more

Questions? Contact me at karen.wetzel@nist.gov
THANK YOU