

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>

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



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

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

NICE Framework Competencies: Moving from Concept to Implementation

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).

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

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

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

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



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

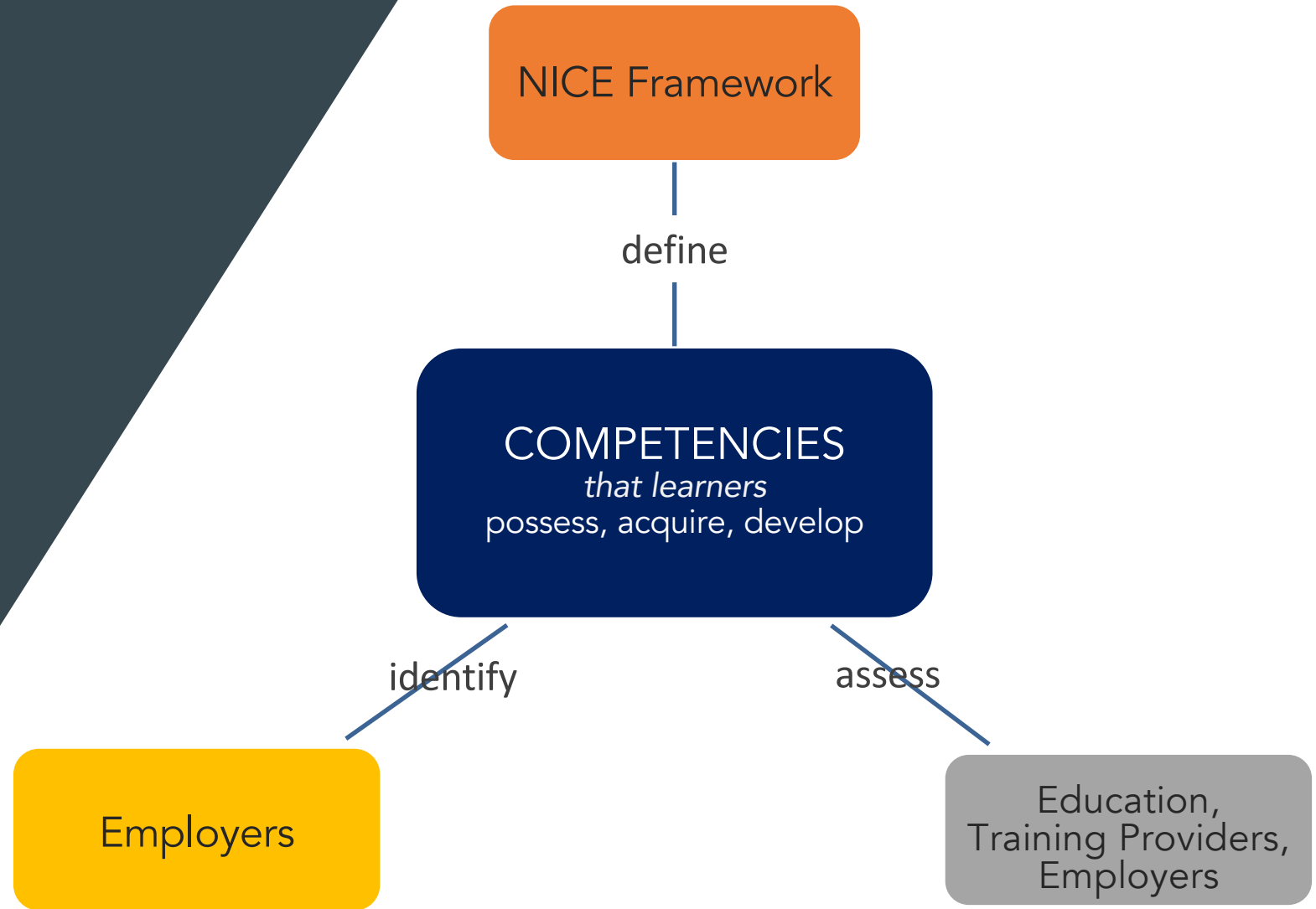
- **Assessment-based hiring and promotion**
- **Identify current gaps and anticipate future needs**
- **Align education and training to organizational goals**

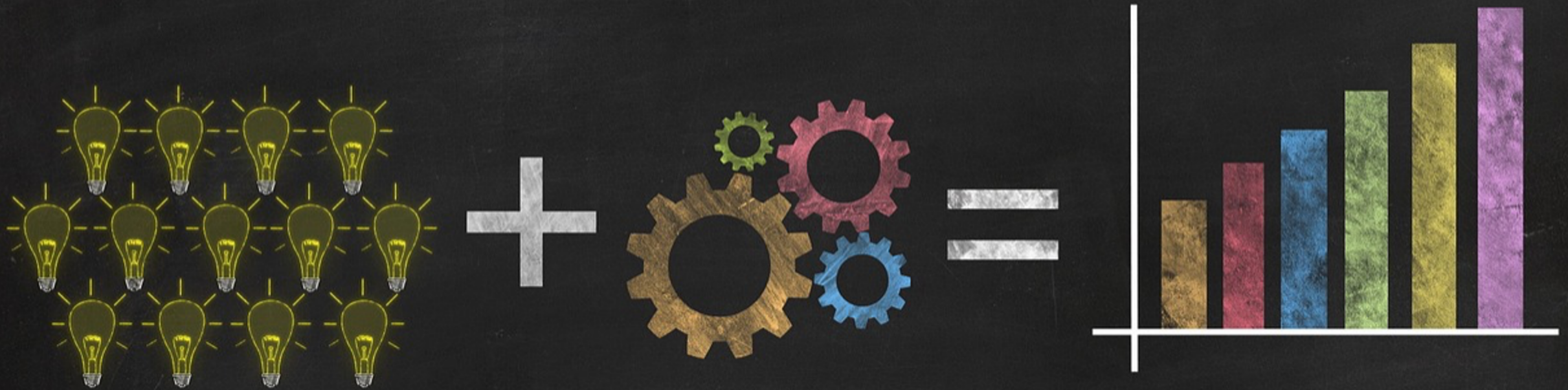
What Competencies Offer

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

Improved Outcomes

Bridge Stakeholders





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...



EMPLOYERS

- Enables the establishment of **regular processes** – from hiring to training and assessment – across an organization.



LEARNERS

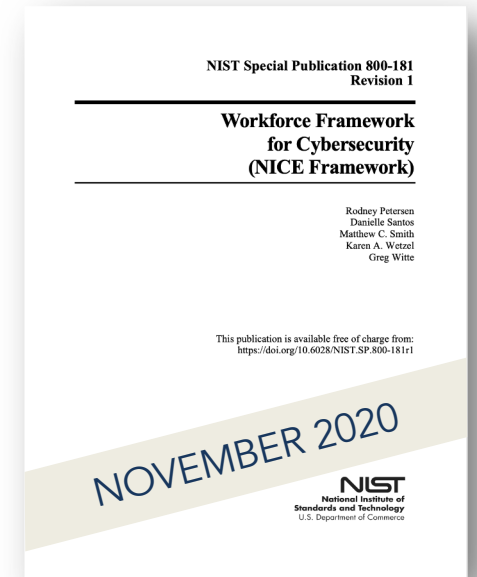
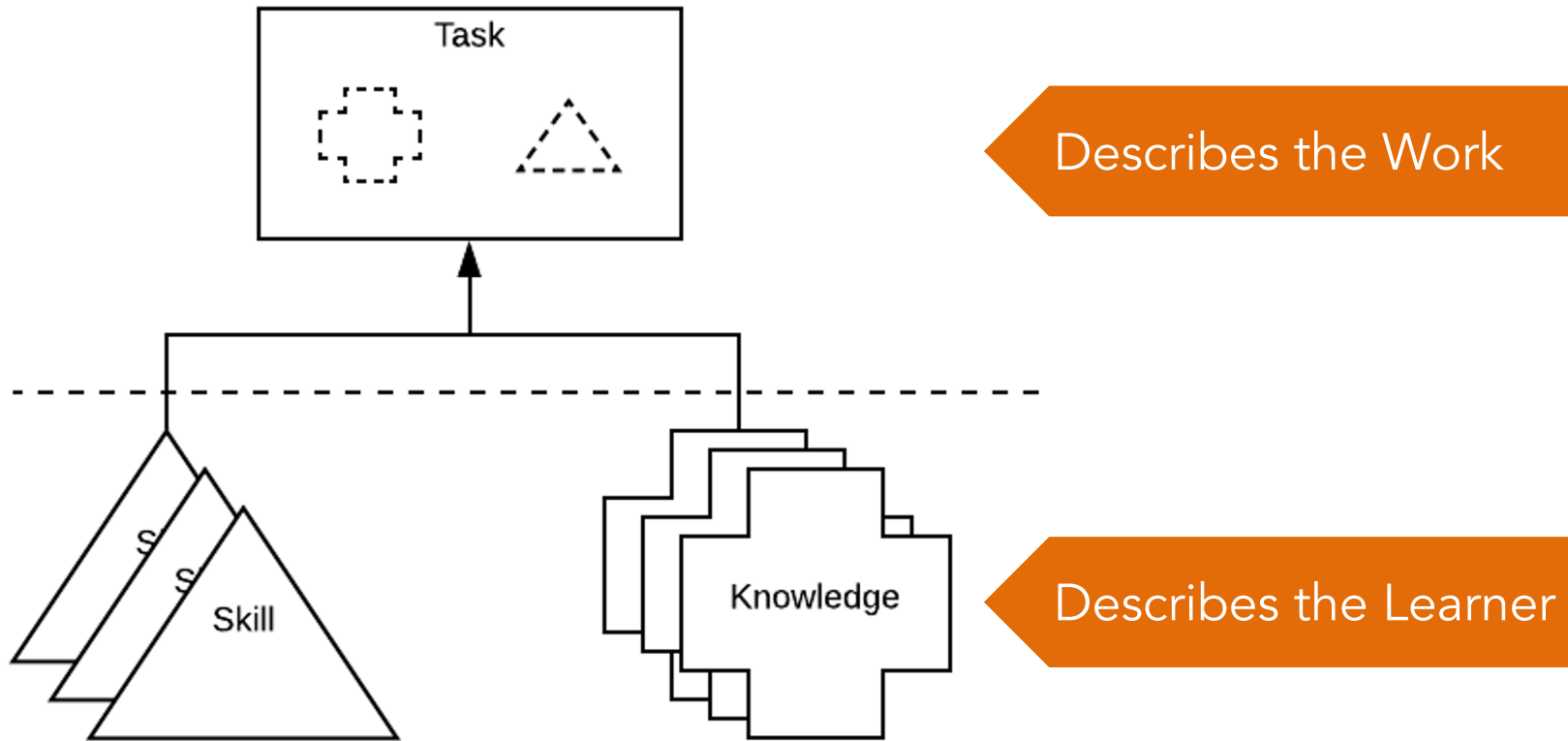
- Shares **clear information about cybersecurity workforce needs** to help students, job-seekers, and workers develop, demonstrate, or improve their competencies.



EDUCATION, TRAINING, & CREDENTIAL PROVIDERS

- 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



nist.gov/nice/framework

Applications and Uses



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](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

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



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

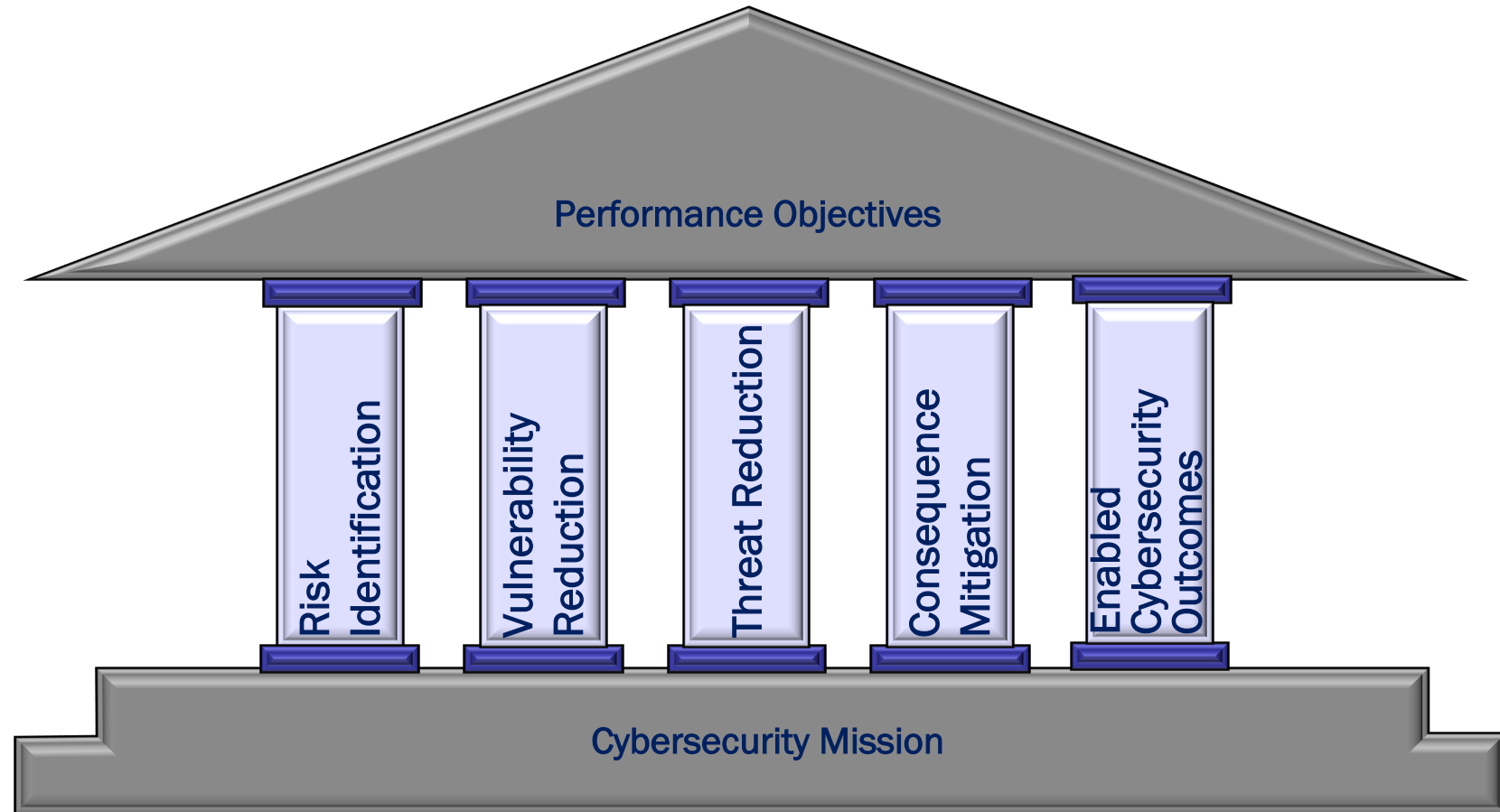


Department of Homeland Security Office of the Chief Human Capital Officer

- 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



Mission-Driven Qualifications



Education and Experience



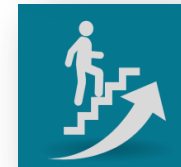
Preferred Degree Types and Certifications



Capabilities



Technical Competencies



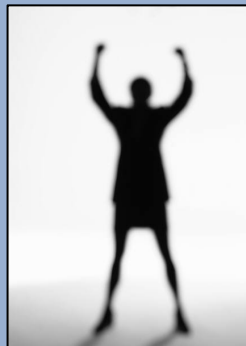
Behavioral Indicators/Benchmarks and Proficiency Levels



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:



- | | |
|----------------------|--|
| <u>My Occupation</u> | → IT 2210 InfoSec Professional (Federal Employee)
Cybersecurity Professional (Private Sector) |
| <u>My Role(s)</u> | → Cybersecurity Analyst (Fed/Private Sector) |
| <u>My Position</u> | → GS-12 Cybersecurity Analyst (Federal Employee)
Associate Cybersecurity Analyst (Private Sector) |
| <u>My Level</u> | → GS 12 (Federal Employee)
Associate (Private Sector) |



Setting Targets and Measuring Proficiencies of Competencies

Competency Definition		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.	
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 <i>(Describes how the competency manifests itself in observable on the job behavior)</i>			
0 No Foundational Knowledge	<ul style="list-style-type: none"> 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 "no proficiency" for purposes of accomplishing work. 		
1 Basic	<ul style="list-style-type: none"> 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. 		
2 Intermediate	<ul style="list-style-type: none"> 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. 		
3 Advanced	<ul style="list-style-type: none"> I have the advanced knowledge and skills necessary in this area for independent use and application in complex or novel work situations. 		
4 Expert	<ul style="list-style-type: none"> 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 		
Criticality			
Importance	Required at Entry	Criticality	
Establishes the significance of the competency to successful performance in the occupation 1 = Not at all Important 5 = Extremely Important	Identifies the competencies required on day 1 of the job versus those that can be learned over time 1 = Not Required 3 = Definitely Required	An evaluation of Importance and Required at Entry ratings to determine which competencies could be used to make personnel decisions	
Proficiency Targets			
Early Career (GS-9/11) Cybersecurity Analyst (Service Desk Analyst)	Tier 1 (GS-12/13) Associate Cybersecurity Analyst	Tier 2 (GS-13/14) Senior Cybersecurity Analyst	Tier 3 (GS-13/14/15) Cyber Threat Analyst (Technical Lead, Expert, Advisor)
<i>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)</i>			

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

Sample tasks to help illustrate the competency.

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



Competency Profiles Drive Competency Assessment & Talent Management



Cybersecurity Analyst Competencies	Cybersecurity Analyst Career Levels			
	Entry/Tier 1 (GS 7 GS 9)	Tier 1 (GS 11 GS 12)	Tier 2 GS 13	Lead GS 14

Illustrative Example

Security Monitoring and Event Analysis	1	2	3	4
Digital Forensics	1	2	3	4
Exploitation Analysis	1	2	3	4
Incident Response	1	2	4	4
Investigation	1	2	2	2
Cyber Threat Analysis	1	2	3	3
Cyber Operations	1	2	3	3



Proficiency Level Targets for Cybersecurity Analyst Career Levels



Competency Profiles Drive Competency Assessment & Talent Management

Illustrative
Example

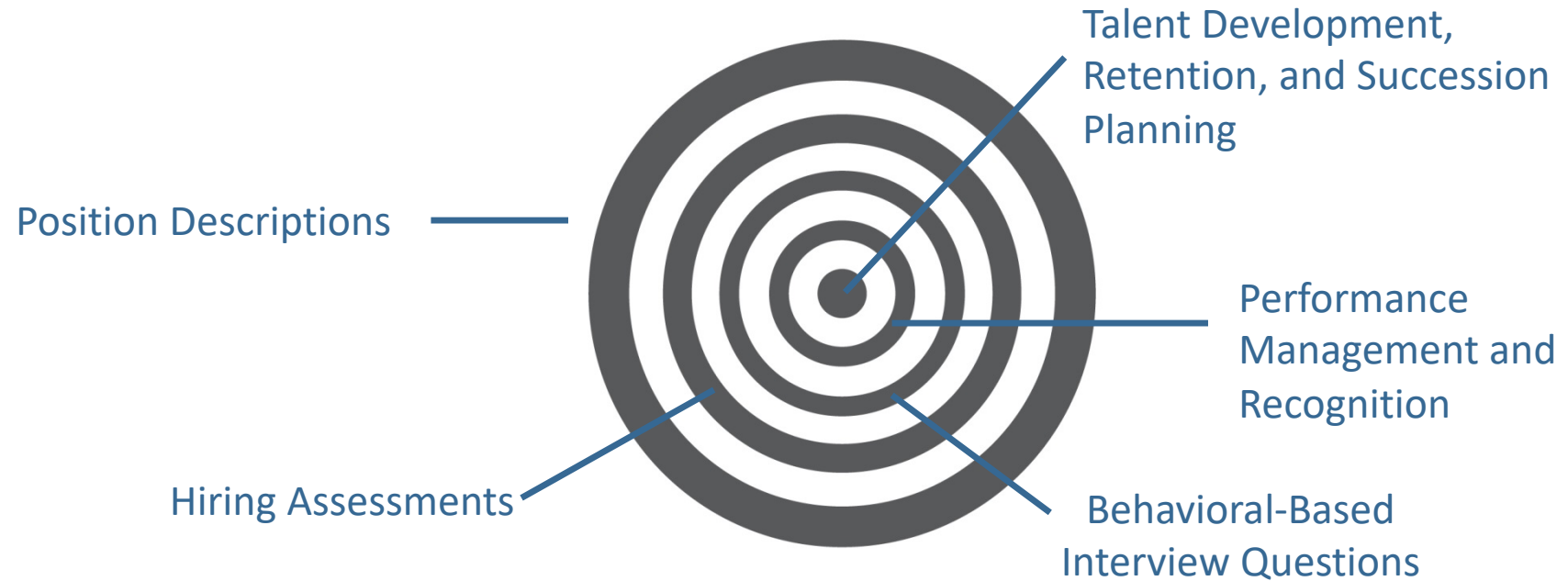
Shared Competencies Among GS-12/ Cybersecurity Specialists, Performing In Different Work Roles	GS-12/ Cybersecurity Specialists			
	Cybersecurity Analyst	Penetration Tester	Security Architect	Policy Lead
Computer Network Defense Analysis	2	3	2	1
Security Monitoring and Event Analysis	2	1	2	1
Digital Forensics	2	3	1	1
Exploitation Analysis	2	3	1	1
Cyber Operations	2	1	1	4

Proficiency Level Targets for Cybersecurity Roles



Proficiency in Practice

Proficiency Targets are Foundational to the Talent Management Lifecycle



Practices of Yesterday & Today

Traditional Practices	Today's Practices
<ul style="list-style-type: none">• Planning for employment for life• Career ladders progressing upward in a linear fashion• Job announcements, branding, outreach, and candidate vetting• Static training classes completed in an ad hoc, reactionary fashion• Off-the-shelf career interest inventories• Success measured by upward progress and increase in salary• In the classroom, formal learning and development offered periodically• Next-level job definition• No integration with succession management, performance management, or L&D• No, or very limited, focus on building personal brand• Doing what you've been told to do and know how to do• Limited career information available• No focus on creating large, diverse talent pools <p data-bbox="499 1036 899 1068"><i>Source: Brandon Hall Group</i></p>	<ul style="list-style-type: none">• Planning for today's gig• Multi-Track career paths with lattices progressing up, down, sideways, and/or in and out• Apps, Buzz Feeds, and "apply now" buttons• Formal mentoring, shadowing, and rotation programs and dedicated attention from senior leaders to "show the ropes"• Personalized skills and capability-based benchmarking assessments• Success measured by perpetual growth in knowledge & experience• On-the-job learning and experience-building offered continuously and supported by relationships and networks• Full career mapping plans for job roles and/or capability areas• Full integration with succession management, performance management, L&D and other talent processes• All about building personal brand• Doing what you are good at and being given the opportunity to learn how to do it better• All career information is widely available and broadcast to all employees across the enterprise• Focused on creating large, diverse talent pools



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?



Recruiting

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



Upskilling

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



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

A person with dark hair and glasses is shown in profile, looking towards the right. They have a thoughtful expression, with their hand resting on their chin. The background is dark, suggesting an office or computer lab environment. A blue can is visible on a desk in the background.

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

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

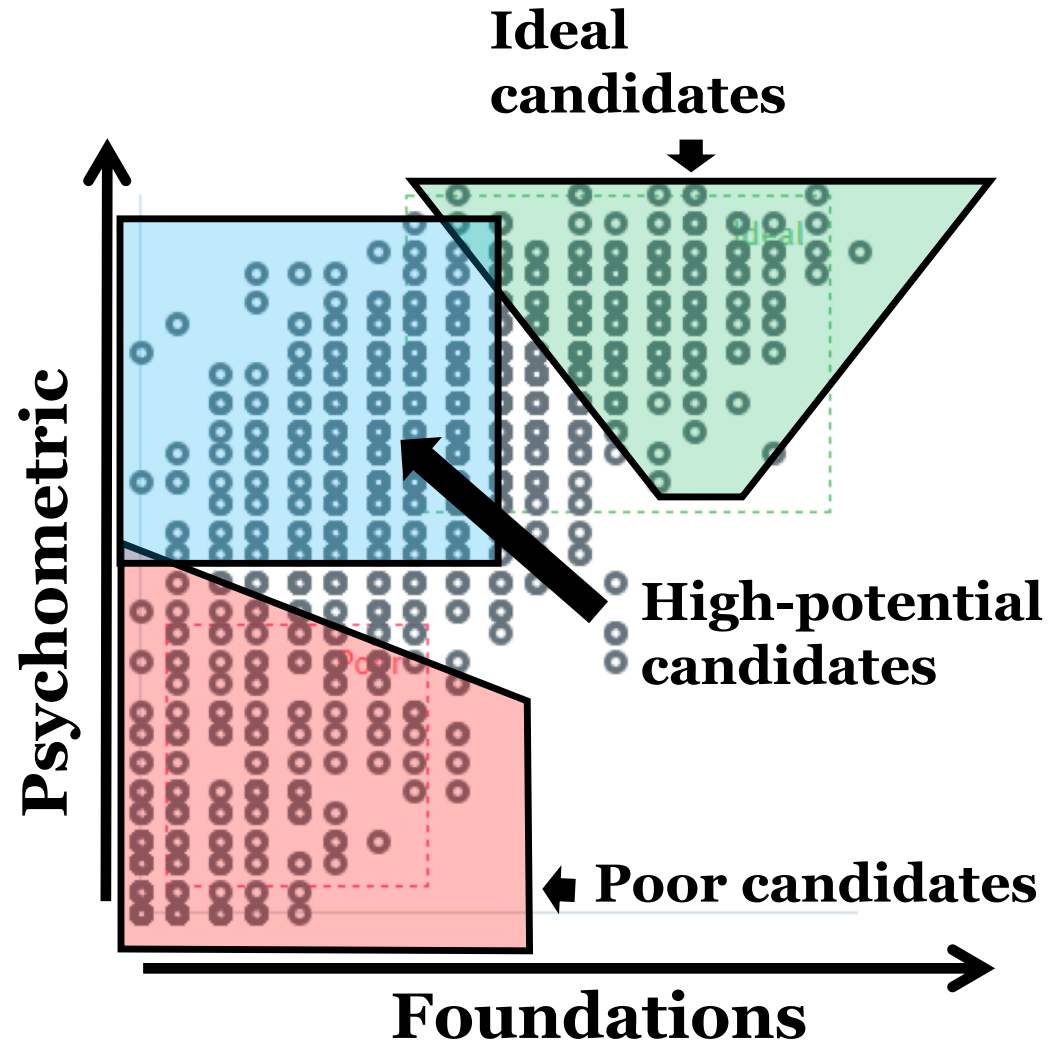
Lower failure rate



Train in cybersecurity for incident response, red teams, defense, and more

More (the hobbyists) were top performers and more also did well

Phase 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



Talent of the Future

*Which of these students can be a cyber star?
Who has curiosity, tenacity, problem solving skills and 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:

	4-year goal	First year	End of 2020
Students assessed in Game	20,000	23,000	200,000
Students taking foundational training	6,000	9,000	38,000
Elite scorers – cyber stars	600	700	4,500



CATAGORY/TOPIC	MODULES
Computer Hardware /Data	6
Linux and Windows	7
Networking	6
Programming	6
Common Attacks & Security	10
Others (Kali, Google, etc)	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?



Recruiting

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



Upskilling

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



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?

A young man with dark hair, wearing large black headphones with orange accents and a blue denim jacket over a white t-shirt, is smiling and looking towards the right. He is sitting at a desk with a laptop in front of him. The background is a blurred green wall with a grid pattern.


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

THANK YOU