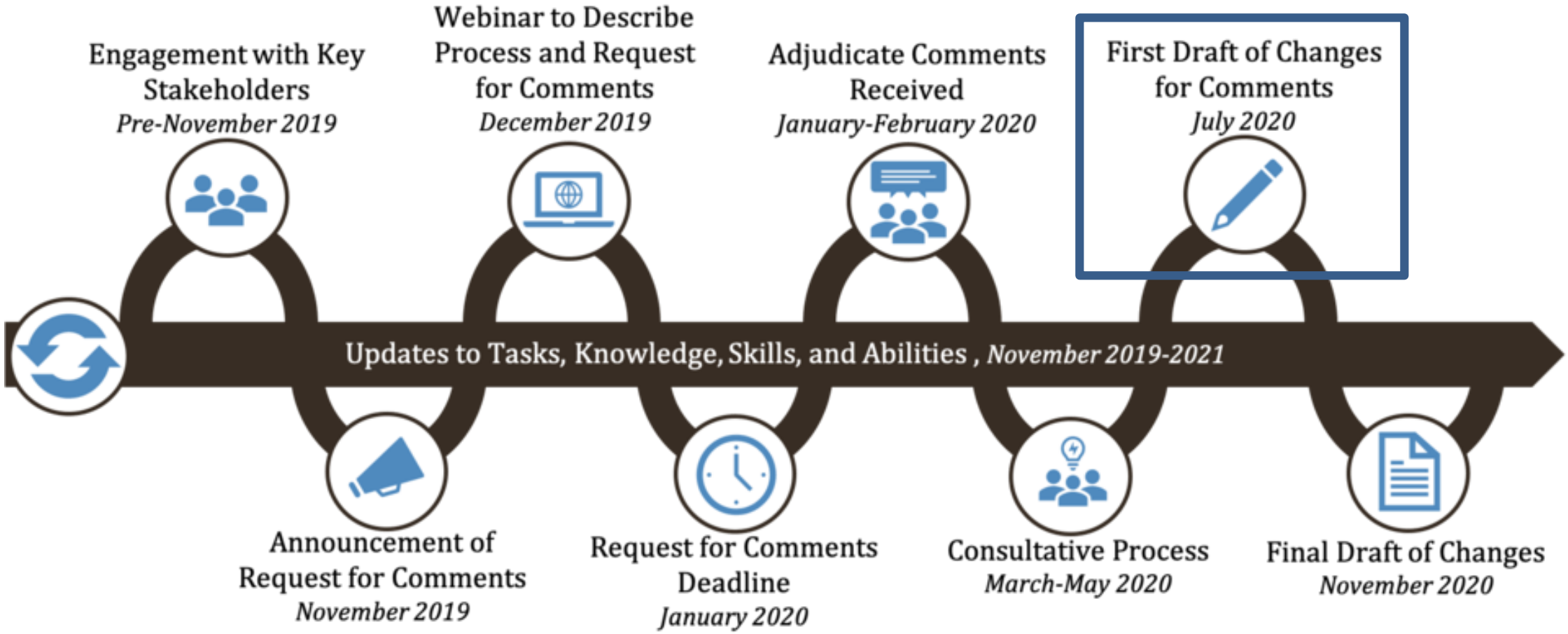
NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

What's New – Revisions to the NICE Framework

July 15, 2020

Timeline of Framework Updates

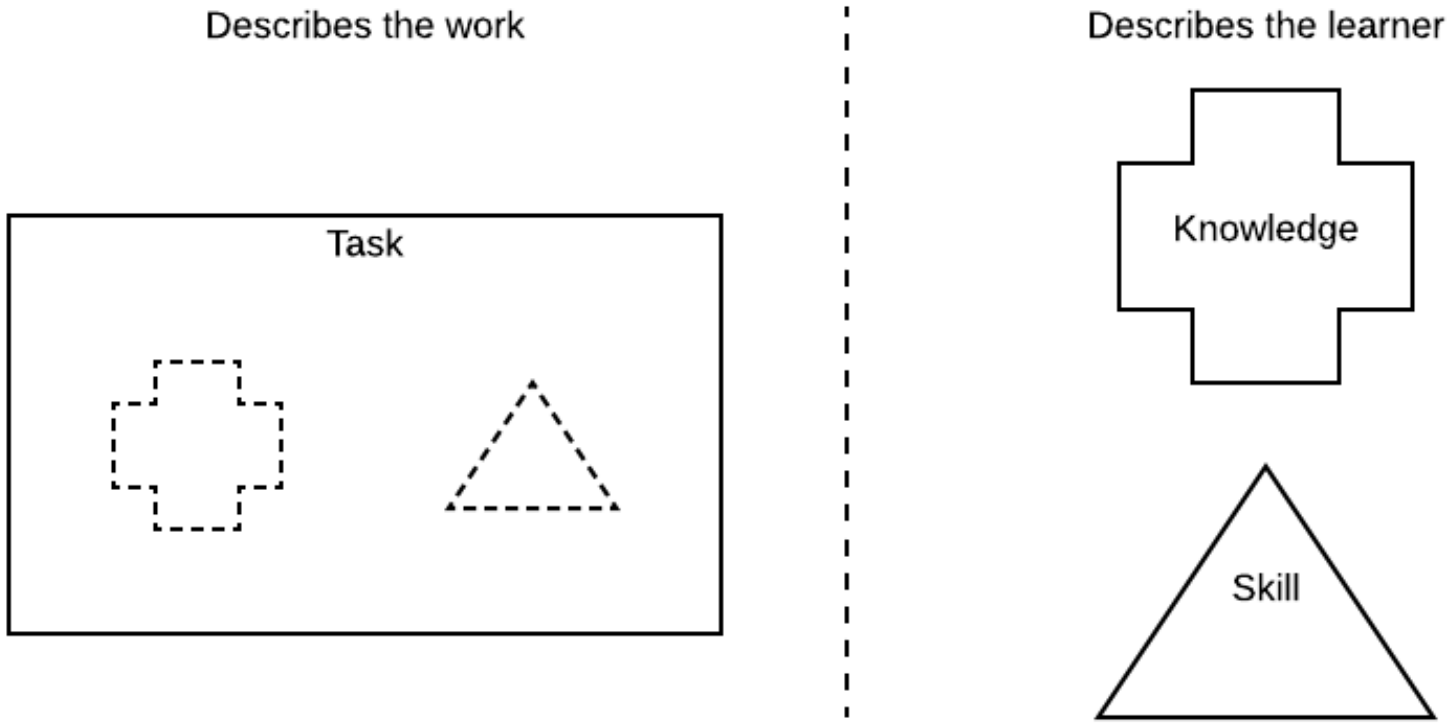


NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Attributes of the New Revision

- **Agility—** The NICE Framework enables organizations to keep pace with a constantly evolving ecosystem.
- **Flexibility—** The NICE Framework enables organizations to account for the organization's unique operating context.
- **Interoperability—** The NICE Framework enables organizations to exchange workforce information using a common language.
- **Modularity—** The NICE Framework enables organizations to communicate about other workforces within an enterprise (e.g., Privacy, Artificial Intelligence , etc.).

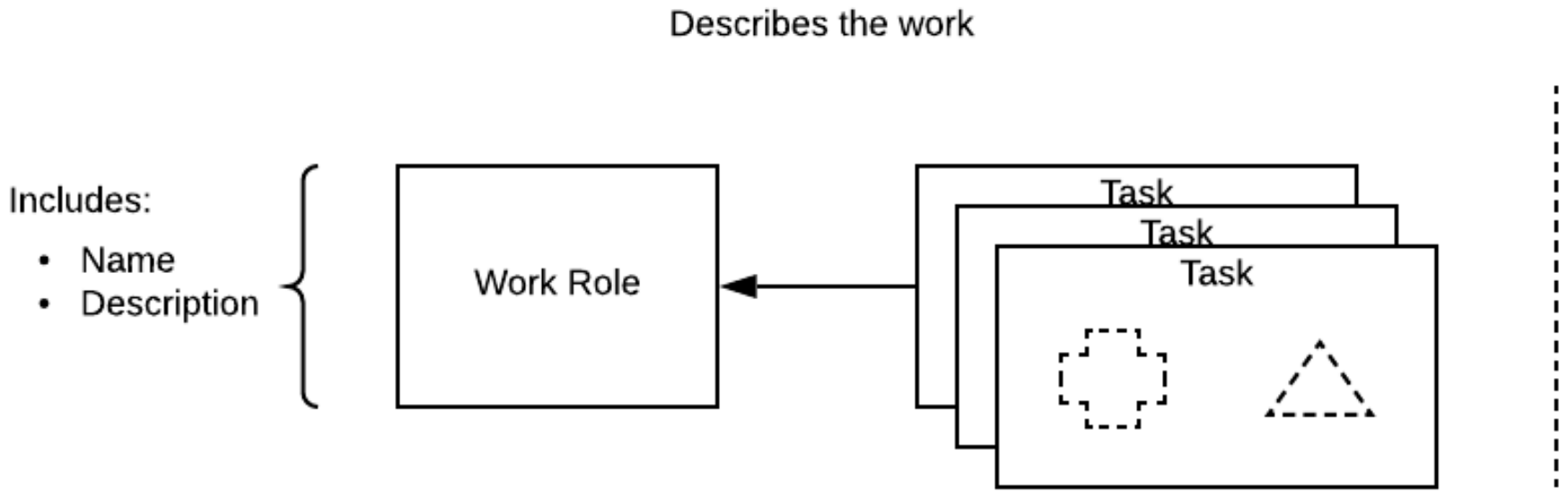
Feature: “The Work” and “The Learner”



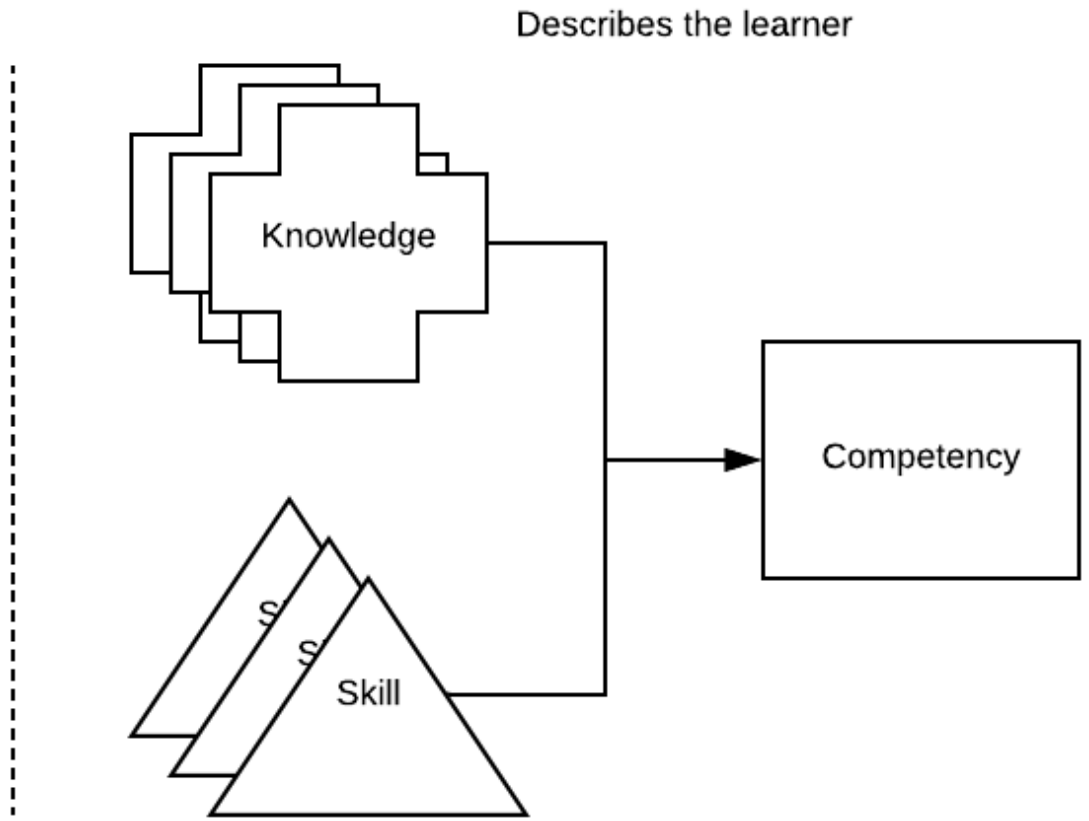
Feature: Building Blocks

- Task: an activity that is directed toward the achievement of objectives
- Knowledge: a retrievable set of concepts within memory
- Skill: the capacity to perform an observable action

Feature: Work Roles



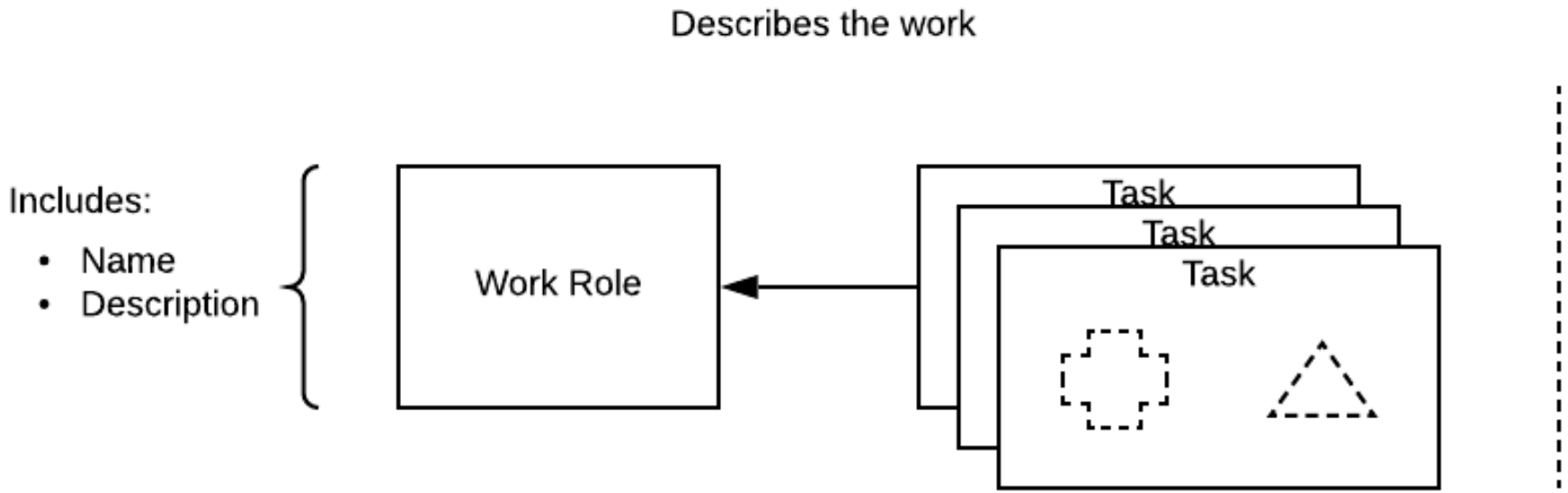
Feature: Competencies



Q & A

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Feature: Work Roles



Pam Frugoli

Senior Workforce Analyst

Employment and Training Administration

U.S. Department of Labor

Use of NICE Framework by Private Sector and Role of Employment and Training Administration

- The Employment and Training Administration (ETA) and industry partners collaborate to develop and maintain dynamic models of the foundation and technical competencies needed in various industries and sectors of the American economy.
- The goal is to promote an understanding of the skill sets and competencies that are essential to educate and train a globally competitive workforce.
- The models are a resource to inform collaboration among industry leaders, educators, economic developers, and public workforce investment professionals to:
  - **Identify specific employer skill needs**
  - **Develop competency-based curricula and training models**
  - **Develop industry-defined performance indicators, skill standards, or certifications**
  - **Develop resources for career exploration and guidance**

DOL-sponsored online resources

Occupational Information Network (O*NET) system

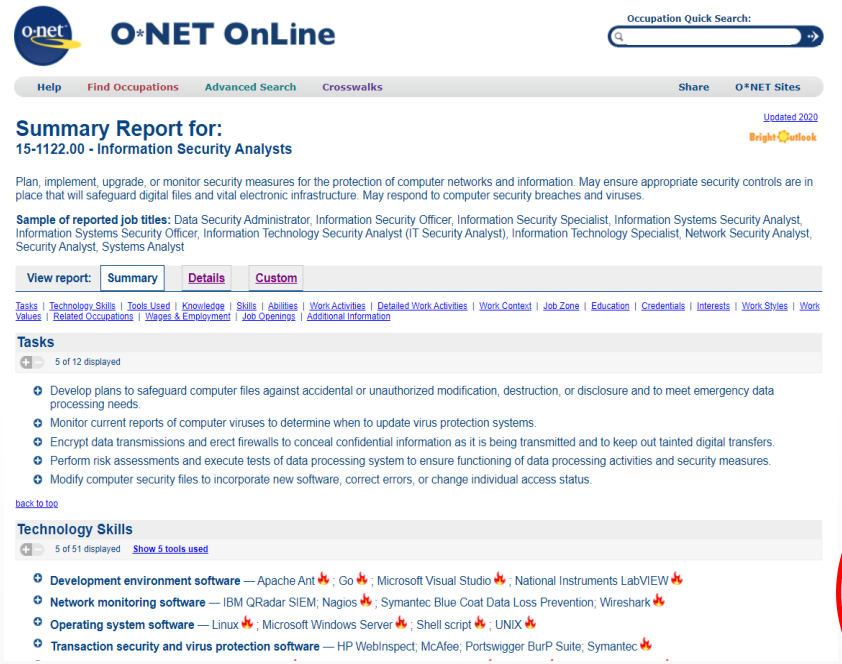
Competency Model Clearinghouse

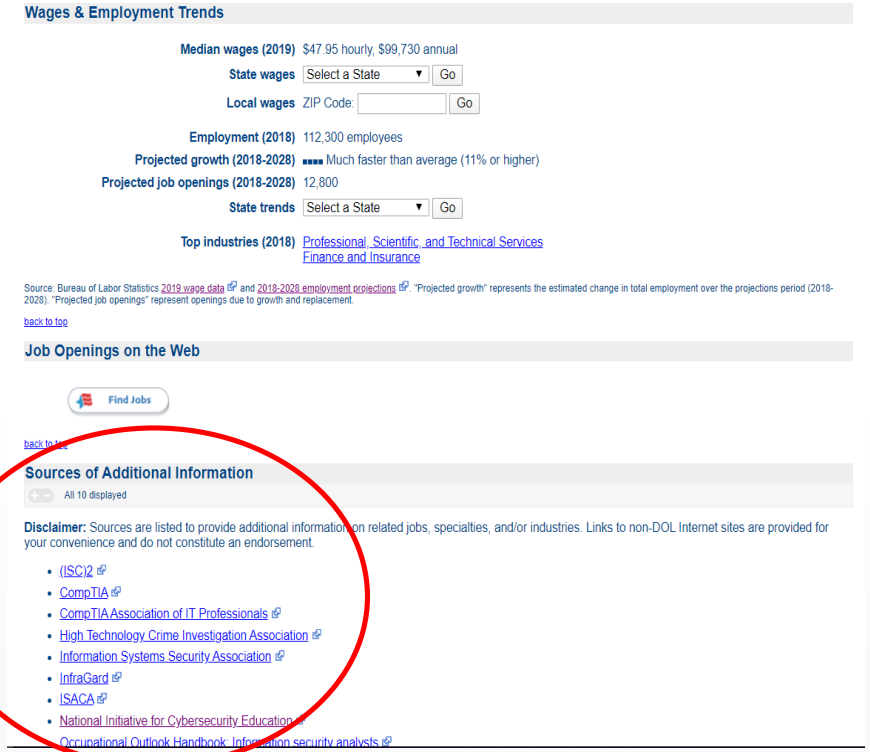
O*NET Focus on Careers and Occupations

O*NET	NICE Cybersecurity Framework
974 Occupations	**52** Work Roles
41 Knowledge Areas	**614** Knowledge statements
35 Skills	**359** Skills
55 Abilities	**119** Abilities
19,566 Tasks	**928** Tasks

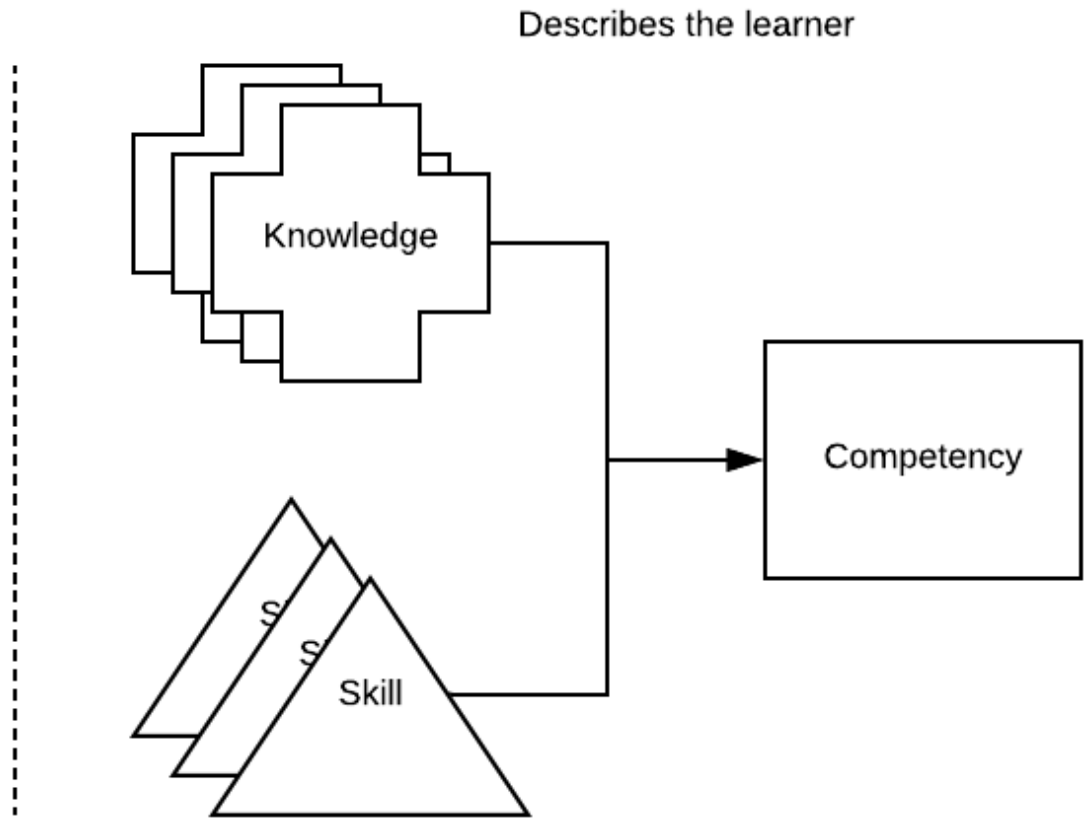
The NICE Framework is an unparalleled **in-depth** resource

O*NET Profile for Information Security Analysts

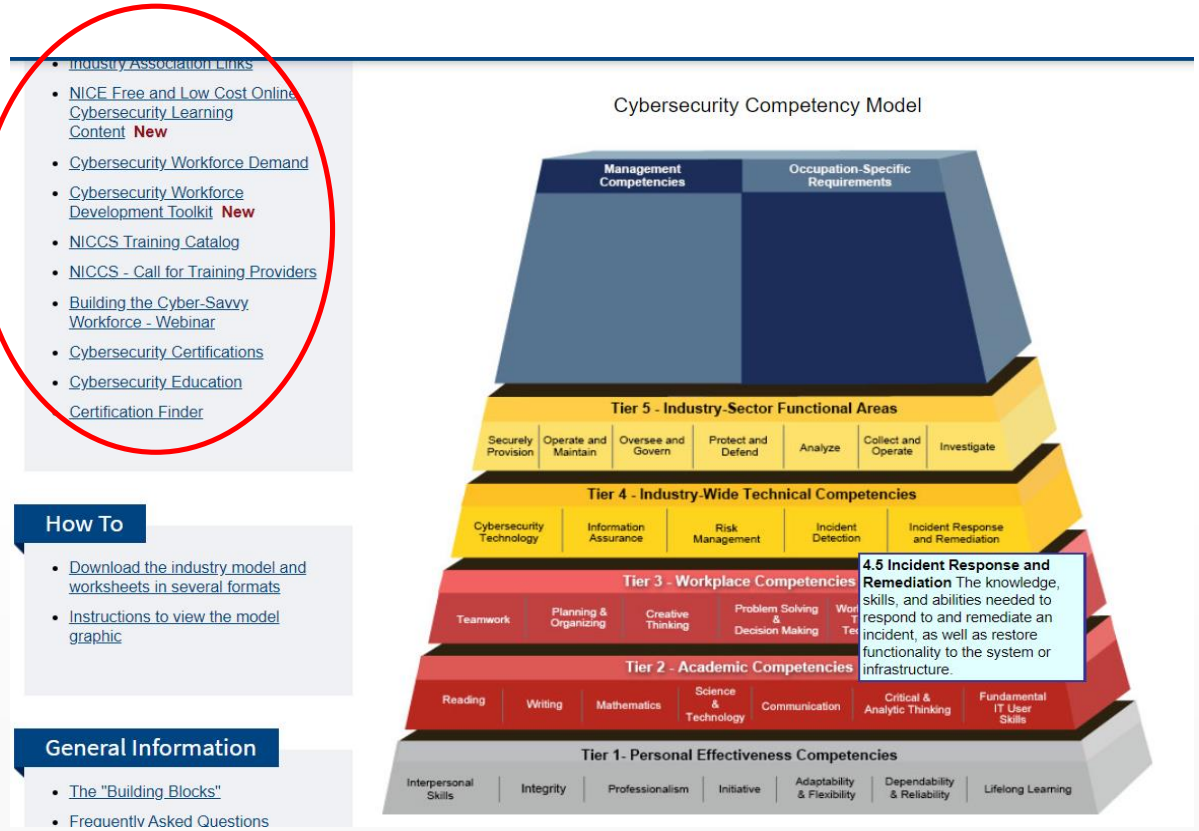




Feature: Competencies



Socializing the NICE Framework to a Wider Audience



https://www.careeronestop.org/CompetencyModel/Competency-Models/cybersecurity

Q & A

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Matthew Isnor

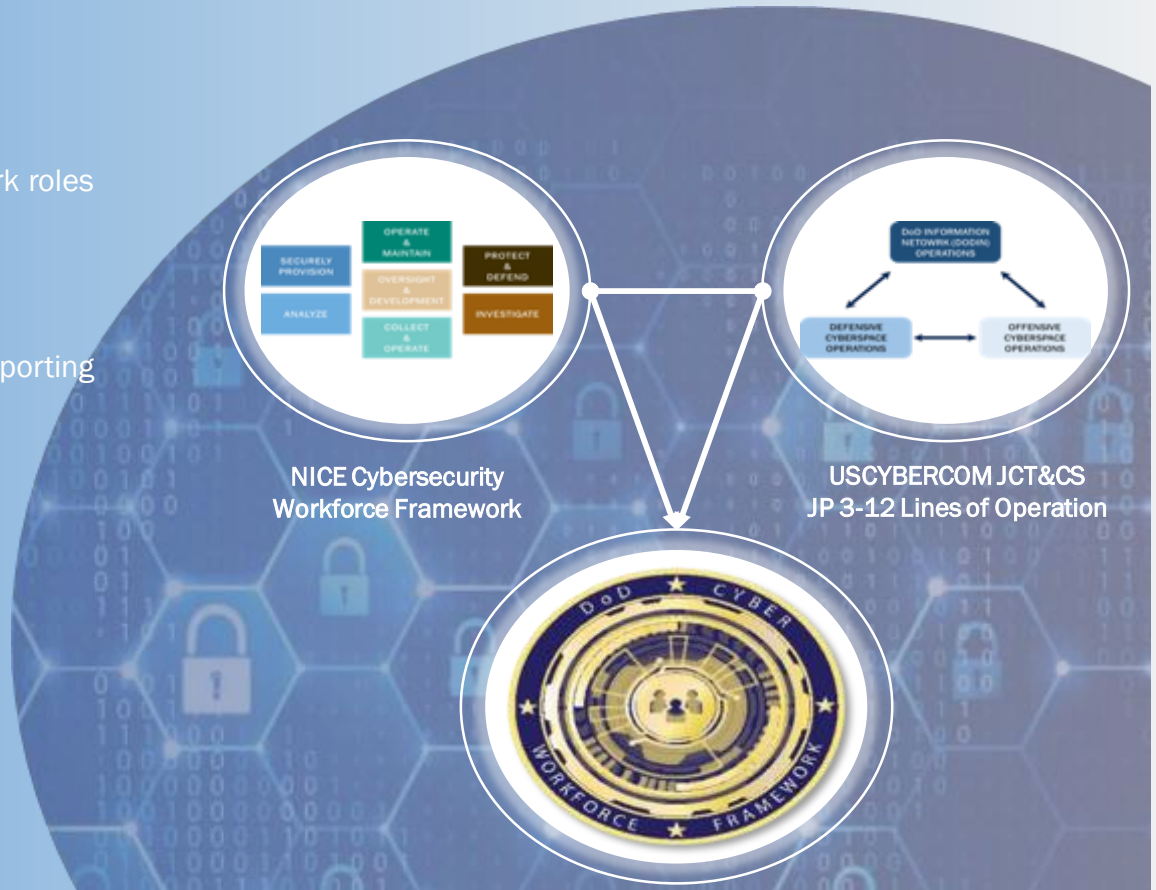
Senior Program Lead

Cyber Workforce Development

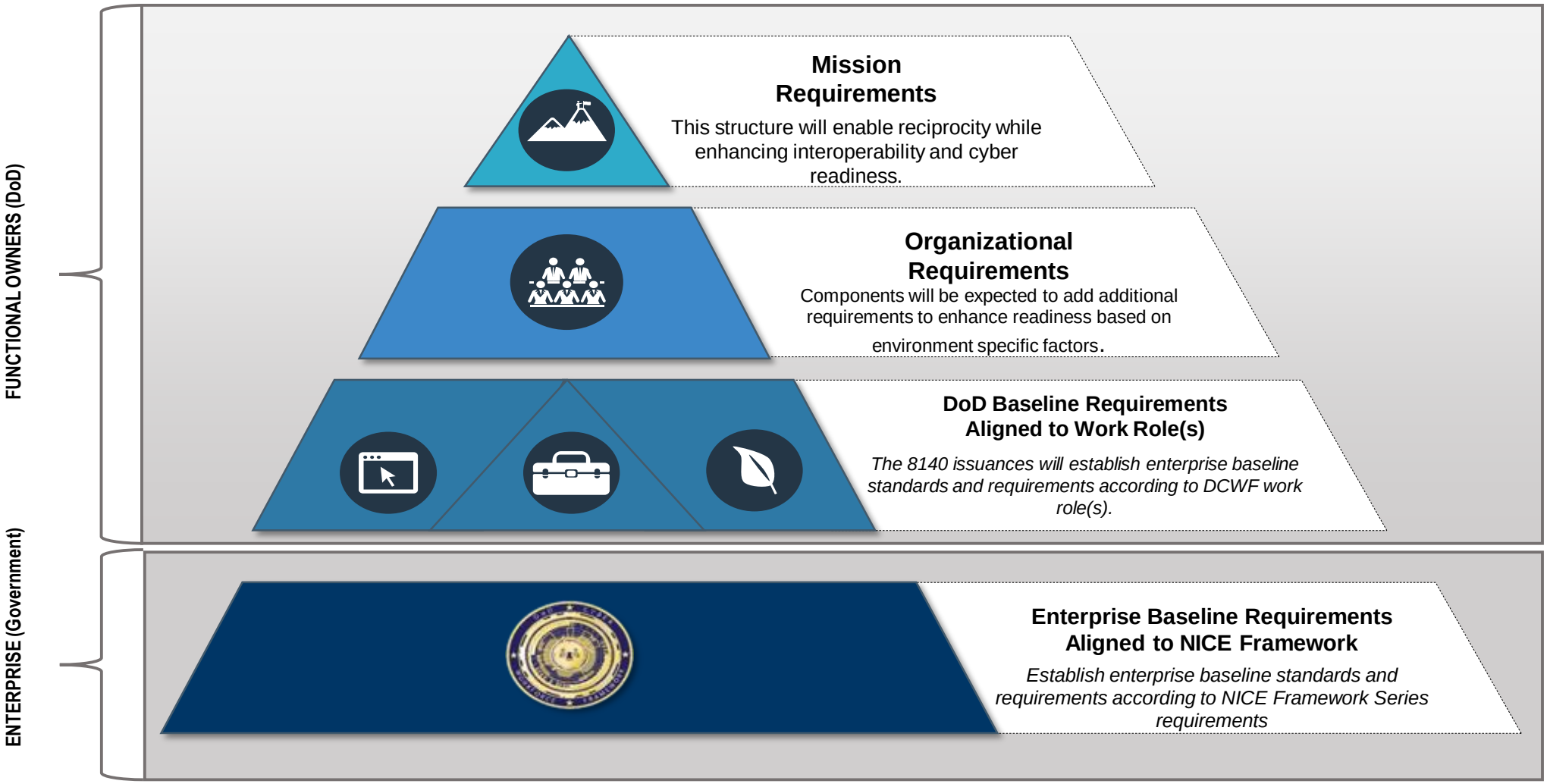
Department of Defense, OCIO

DoD Cyberspace Workforce Framework (DCWF)

- Establishes an authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator
- Develops qualification requirements for cyber work roles outlined in DoD Manual 8140.XX
- Facilitates uniform identification, tracking, and reporting required by the Federal Cybersecurity Workforce Assessment Act (FCWAA)
- The DCWF has been adapted at the national level in NIST Special Publication 800-181
- Used to develop an international framework under the NATO Multinational Cyber Defense Training & Education Project.



DoD Organizational Building Blocks



Lisa Dorr, Senior Talent 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 Manager for Strategic Analysis & Change Management and Talent Engagement & Development

Federal Cybersecurity Workforce Trends

Workforce Trends

1. *Government work is increasingly knowledge work, requiring complex problem-solving and unpredictable application of skills*
+
2. *Jobs are becoming increasingly non-standard and complex*
+
3. *Employee expectations no longer always map to the 30-year federal career*
+
4. *Highly-competitive labor markets exist in which the Federal Government is only one employer*

Practices to Revisit

1. *Position classification from the first half of the 20th century cannot describe cybersecurity work or talent*
+
2. *Self-rating and brief interviews cannot measure cybersecurity expertise*
+
3. *Rigid, tenure-based approaches to pay and career progression are not competitive*

DHS Cybersecurity Talent Management System

Background

Congress granted the Secretary broad authority to establish an alternative personnel system to recruit and retain cybersecurity talent

- *Passed as part of the December 2014 Border Patrol Agent Pay Reform Act*
- *Broad authority with some restrictions and requirements, including producing regulation*
- *Similar language to authorities for personnel systems in Department of Defense and Intelligence Community*

Challenge

Simply eliminating a step in the hiring process or adding a pay grade will not make DHS competitive, especially given the global shortage for cybersecurity talent

- *Department's cybersecurity human capital challenges are about more than just pay*
- *The world of work—especially cybersecurity work—continues to evolve*
- *Conventional civil service approaches, including position-based hiring and pay, are showing their age*

Solution

DHS is preparing to launch the CTMS and Cybersecurity Service (DHS-CS) to better manage cybersecurity talent in the 21st century

- *Modernize talent management to align to and keep pace with cybersecurity work*
- *Take a comprehensive, mission-focused approach to recruit and retain talent*
- *Understand and customize leading private and public sector practices for DHS*

Methodology

Sourced input from key DHS cybersecurity and human capital stakeholders + *Reviewed all major federal personnel transformations since the 1970s* + *Benchmarked leading private sector practices, including those for hiring assessment and compensation* + *Engaged with human capital experts from the Office of Personnel Management and the Intelligence Community*

Ken Vrooman, Senior Advisor

Cybersecurity and Infrastructure Security Agency

- Cyber Defense Education and Training sub-division
- Acting Branch Chief for the Curriculum, Evaluation and Support Branch

Cyber Defense Education & Training

- As the Nation's Risk Advisor, CISA leads the effort to ensure there is an appropriate staffing of cybersecurity professionals to address the increasing demand of protecting the government, critical infrastructures, SLTT, and public/private partners.
- To accomplish this, CISA is standing up the Cyber Defense Education & Training (CDET) Subdivision to consolidate and expand the agency's ability to address this workforce shortage crisis.

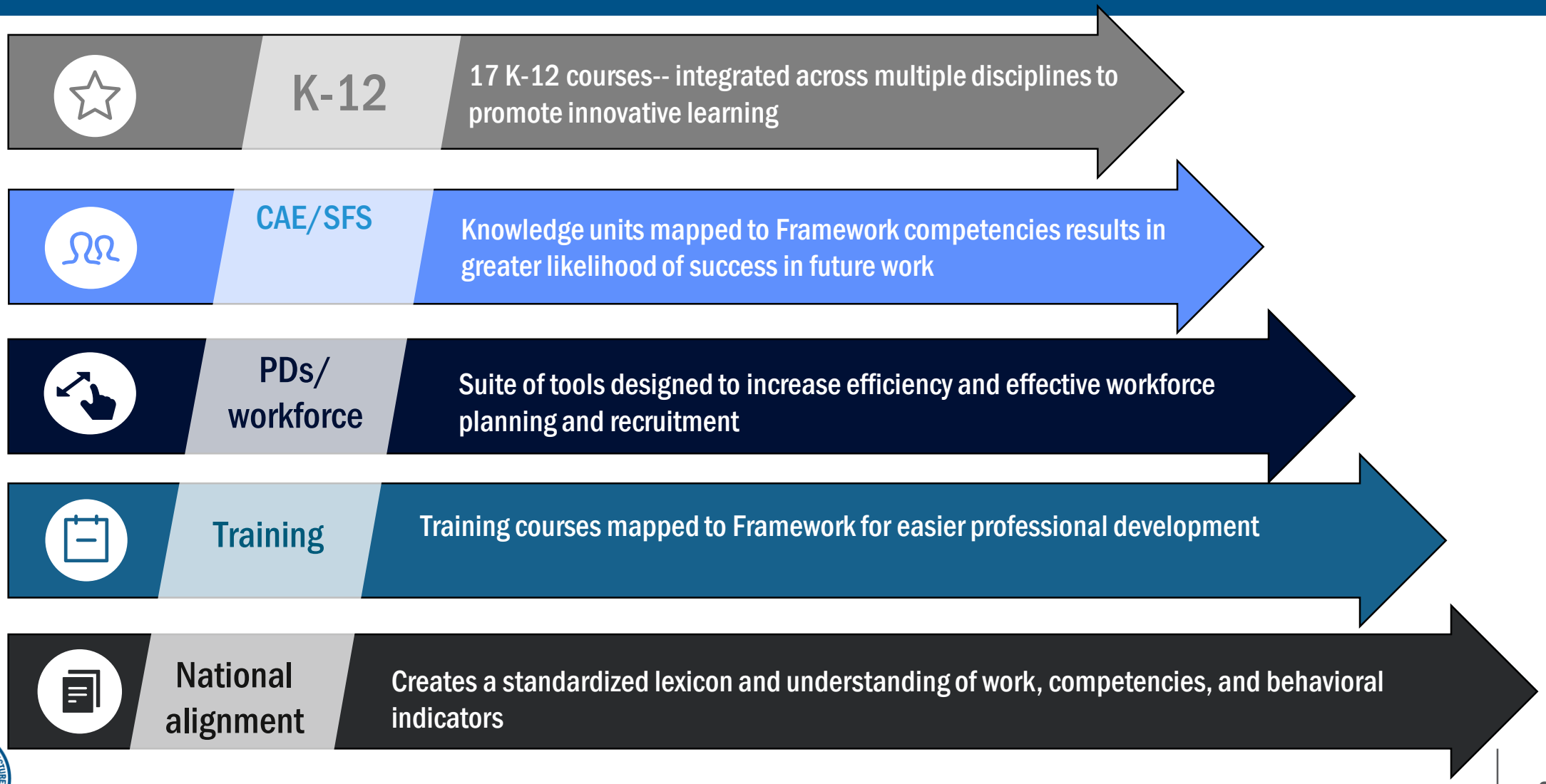
CDET Mission

Educating the Nation to Address Cybersecurity Challenges

CDET Vision

Sustain an Adaptive Cybersecurity Workforce as a National Asset

NICE Framework is the Core



Feature: Building Teams with Work Roles

Lifecycle Phase	Work Role
Design	Security Architect
Build	Software Developer
Deploy	Network Operations Specialist
Operate	Customer Support Specialist
Maintain	Database Administrator
Decommission	Communications Specialist

Feature: Building Teams with Competencies

- Example: Red Team
  - Competency: Engagement Planning
  - Competency: Rules of Engagement
  - Competency: Pen Testing
  - Competency: Data Collection
  - Competency: Vulnerability Exploitation

Q & A

Thank You for Joining Us!

Upcoming Webinar: *Educating Youth for a Cybersecurity Future*

When: Wednesday, September 16, 2020, at 2:00 p.m. EDT

Register: https://nist-nice.adobeconnect.com/webinarsep2020/event/registration.html

nist.gov/nice/webinars

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION