

# Strengthening the Nation's Cybersecurity Workforce

**Rodney Petersen**

Director,

National Initiative for Cybersecurity Education (NICE)

*October 26, 2021*

To energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development

# Values



Foster communication



Facilitate collaboration



Share and leverage resources



Act based on evidence



Evaluate and improve



Challenge assumptions



Stimulate innovation

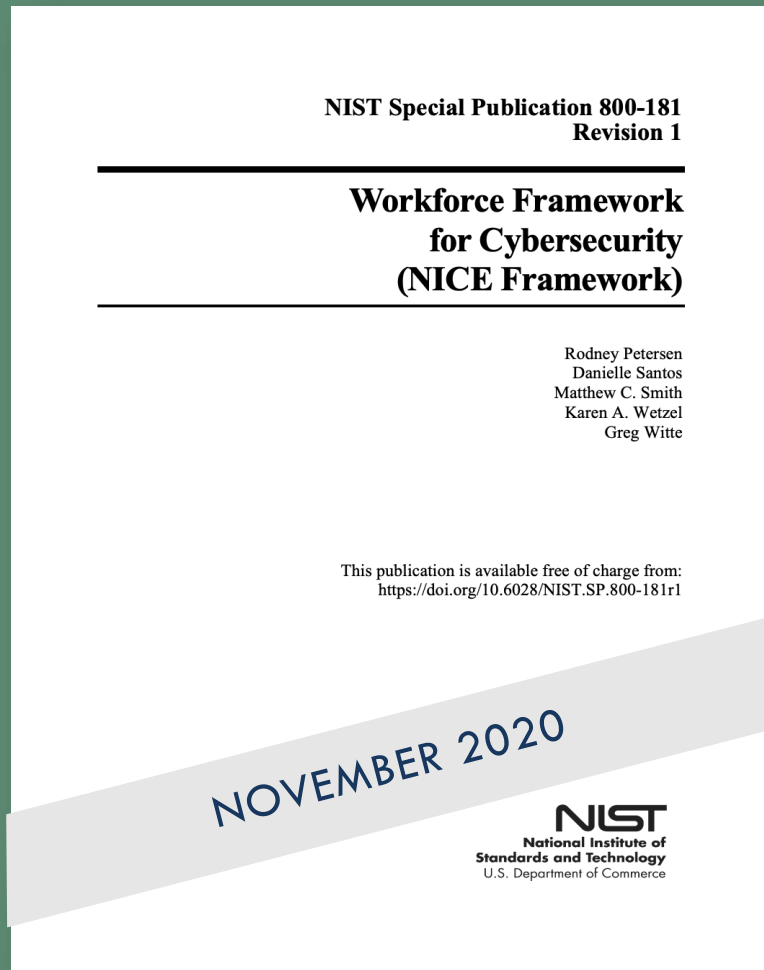


Model inclusion

# Goals



# Workforce Framework for Cybersecurity (NICE Framework)

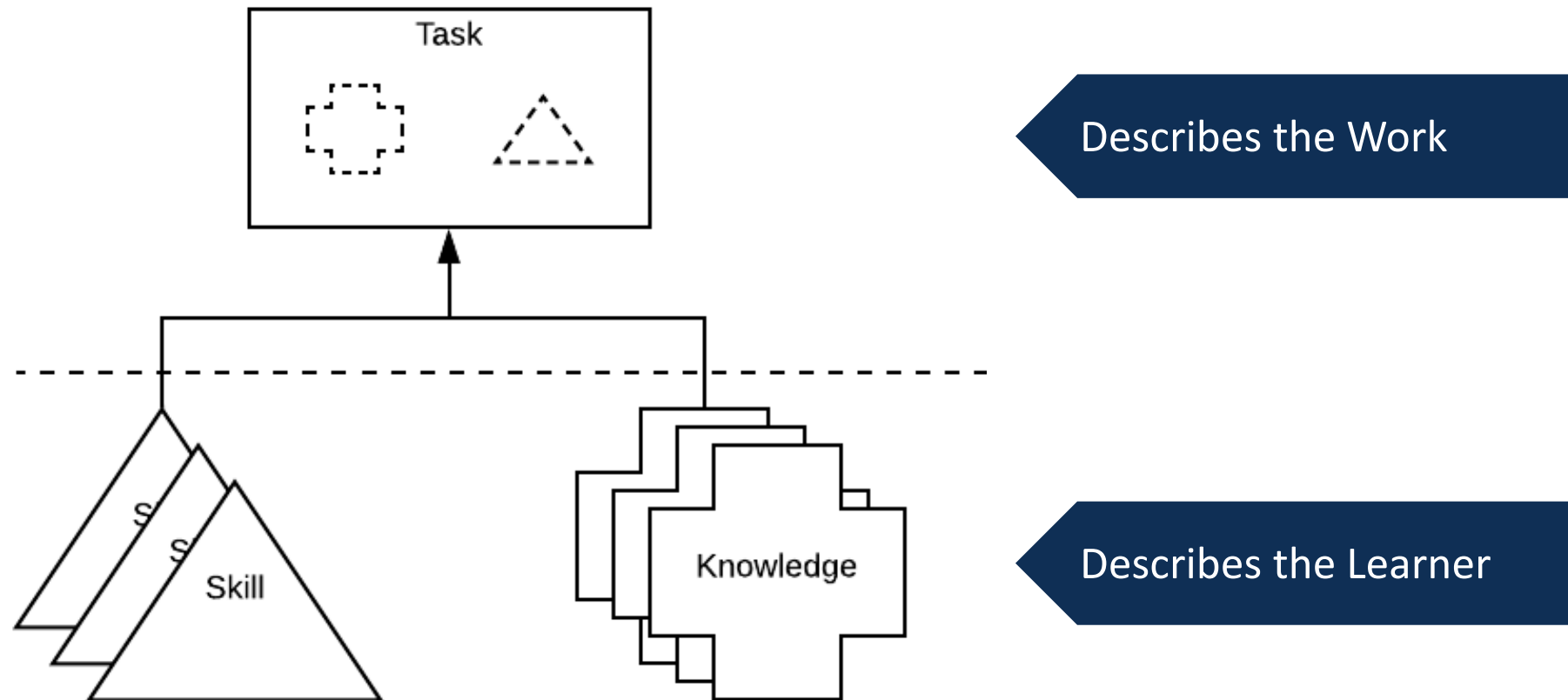


- Title: Workforce Framework for Cybersecurity
- Introduction of Competencies
- Removed:
  - Specialty Areas (reflected in Competencies, Work Roles)
  - Ability Statements (incorporated in Skill statements)
- Appendices: Moved outside the publication

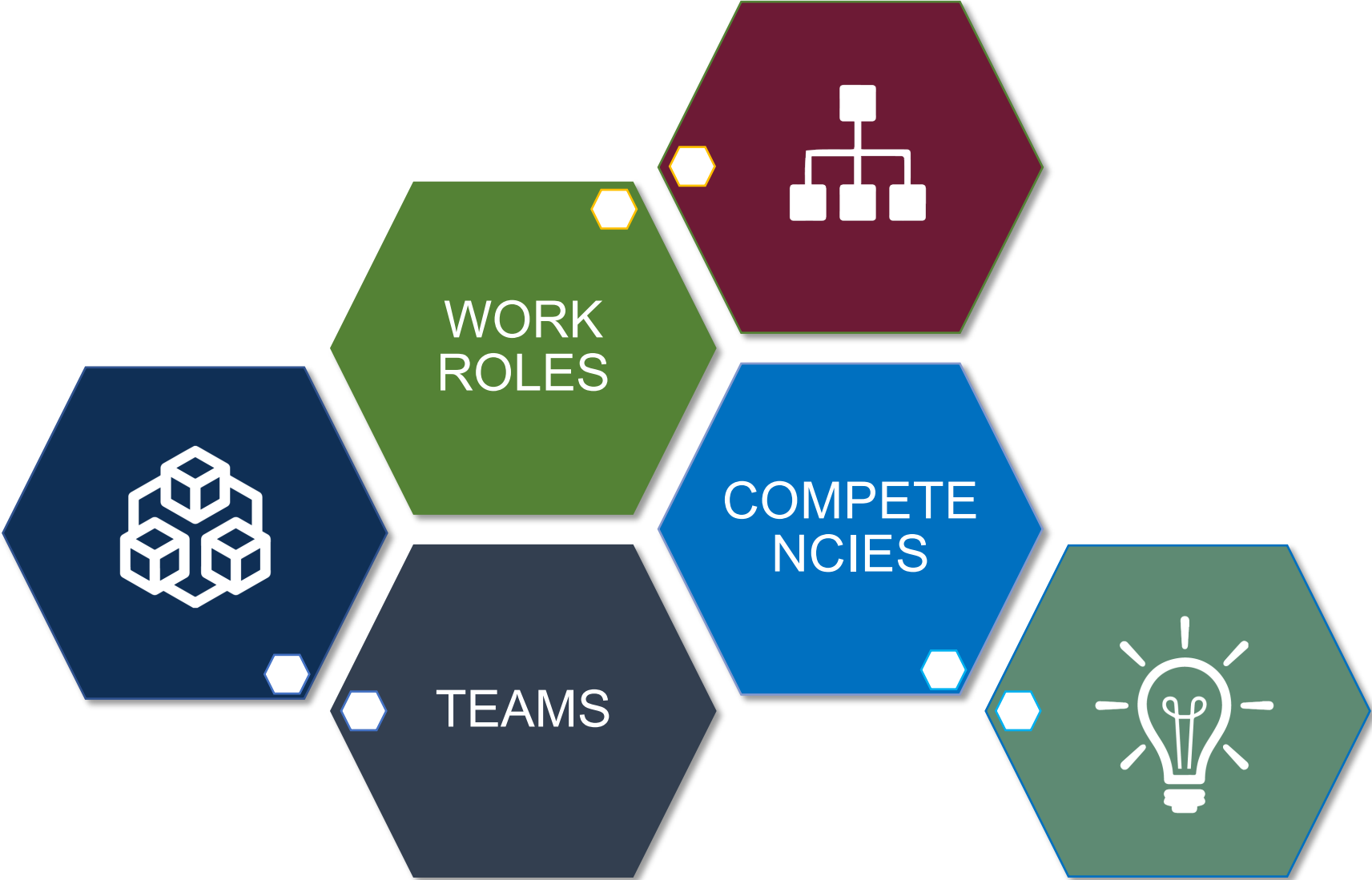
[nist.gov/nice/framework](https://nist.gov/nice/framework)

# Core Building Blocks

## Building Blocks: Tasks, Knowledge, and Skills (TKS)



# Applications and Uses





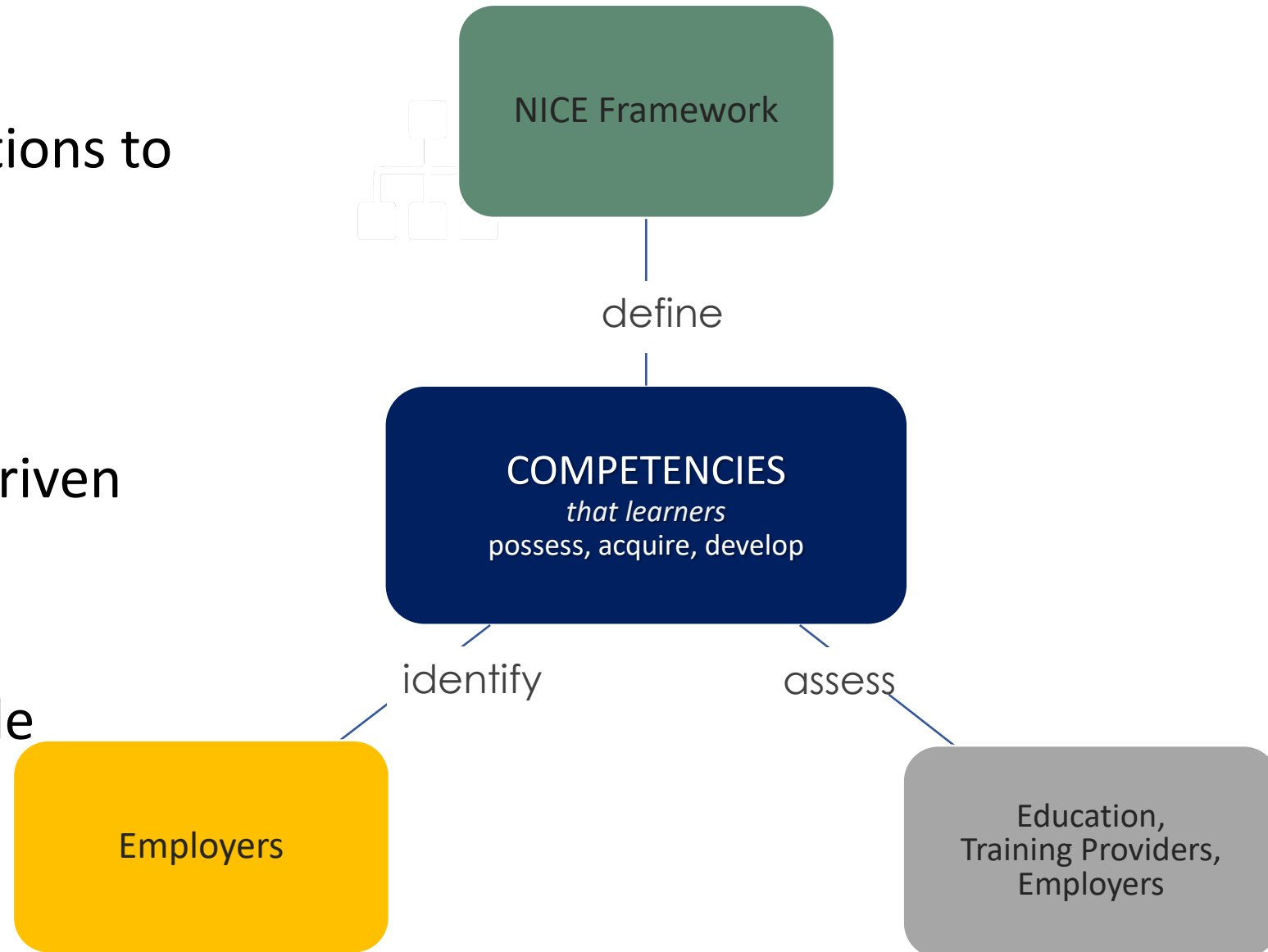
# NICE Framework Competencies

## Competency

- A mechanism for organizations to assess learners.

## Competencies are

- Defined via an employer-driven approach
- Learner-focused
- Observable and measurable





## Model Framework Structure

- Building Blocks
- Sample Uses
- Optional Components



## A Workforce Framework Template



## Guidance on How to Write TKS statements, Competencies, and Work Roles



## Effective Practices for Workforce Framework Development and Stakeholder Engagement

- About the Framework
- Current Version & Latest Updates
- Resources
  - By Stakeholder
  - Users Group
  - Success Stories
  - Framework in Focus
  - Presentations



# NICE Framework Success Stories

**NICE FRAMEWORK SUCCESS STORY**  
Cybersecurity Curricula, Morgan State University

Create Learning Outcomes

The voluntary **Workforce Framework for Cybersecurity (NICE Framework)** was developed through a collaborative process by industry, academia, and government stakeholders. It establishes a taxonomy and common lexicon that describes cybersecurity work and is intended for use in both the public and private sectors. NIST does not validate or endorse any individual organization or its approach to using the NICE Framework.

**ORGANIZATIONAL PROFILE**

Morgan State University is the premier public urban research university in Maryland, known for its excellence in teaching, intensive research, effective public service and community engagement. Morgan prepares diverse and competitive graduates for success in a global, interdependent society.

The National Security Agency (NSA) and the U.S. Department of Homeland Security (DHS) have designated Morgan State University as a National Center of Academic Excellence in Cyber Defense Education (CAE-CD). Cybersecurity courses at Morgan have been mapped to the CAE Knowledge Units and NICE Framework with the help of a cybersecurity curriculum development tool developed by funding from NSA.

Cybersecurity education at Morgan covers a variety of areas in computer science, computer engineering, and information systems. Morgan Computer Science provides a solid foundation in theoretical computer science as well as applied engineering, artificial intelligence/data science, and robotics.

**DRIVERS**

- Gaps between cybersecurity learning and workforce development.
- Lack of hands-on skills.
- The need of a pipeline of students to study cybersecurity, for internships, and to work for cybersecurity companies.
- Alignment of learning with CAE designation and industry needs.

- Demonstration of artificial intelligence (AI)-enabled cybersecurity curriculum development tool.
- Preparation of next-generation cybersecurity warriors to take on the challenges and threats in cyberspace.

**PROCESS**

Course Development: Top Down and Bottom Up

Course development using the NICE Framework was approached from both the top-down and bottom-up. For cybersecurity class COSC 351, we went top-down, working from Specialty Area to Knowledge, Skills, and Abilities (KSAs), and then mapped to the Vulnerability Assessment Analyst Work Role. Later, the AI tool reminded us to add pen test in order to obtain a strong "mapping".

Figure 1: AI engine on AWS for cybersecurity curriculum development

**NICE FRAMEWORK SUCCESS STORY**  
Innovation Challenge, Cal Poly California Cybersecurity Institute

**BENEFITS & IMPACT**

2020 CCIC was particularly unique to our institution. Upon graduating high school, one of our top high school competitors began an internship at CCI and has had an active role in the 2020 competition. His experience as a past competitor has been a valuable asset to our team.

Our goal is to expose more students from underserved communities to a career in cybersecurity through the NICE Framework by participating in the CCIC. We are tracking the success of our student participants and how this challenge has inspired students to explore a cybersecurity career.

January 2021

**NICE**  
NATIONAL INSTITUTE FOR CYBERSECURITY EDUCATION

- Organizational Profile
- Drivers
- Process
- Tie in with the NICE Framework
- Benefits & Impact

<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/success-story-catalog>

## NICE FRAMEWORK RESOURCE CENTER

- About +
- Current Version +
- Latest Updates
- Resources** -
- Users Group
- Employer Resources
- Education and Training
- Provider Resources
- Learner Resources
- Success Stories +
- Framework in Focus**
- Presentations

## Framework in Focus

To help increase the visibility of the National Initiative for Cybersecurity Education (NICE), the NICE Program Office issues [quarterly eNewsletters](#). Each newsletter contains a profile of a cybersecurity practitioner to illustrate application of the NICE Framework Categories, Specialty Areas, and Work Roles.

Interviews are recorded and transcribed. Click any of the links below to listen to the audio and download the transcripts.



SECURELY PROVISION



OPERATE & MAINTAIN



OVERSEE & GOVERN



PROTECT & DEFEND



ANALYZE



COLLECT & OPERATE



INVESTIGATE

# Framework in Focus

## NICE FRAMEWORK R

About +

Current Version +

Latest Updates

**Resources** -

Users Group

Employer Resources

Education and Training

Provider Resources

Learner Resources

Success Stories +

**Framework in Focus**

Presentations



**Chris Knox**

Manager, Security Awareness & Analysis, CPS Energy

*NICE Framework Work Roles: Cyber Instructor/Threat Analyst*

[Listen to the Interview](#)



**Lonnie Harris**

Director, Security Enterprise Engineering, Equifax, Inc.

*NICE Framework Work Roles: Security Architect/Systems Developer/Cyber Defense Analyst*

[Listen to the Interview](#)



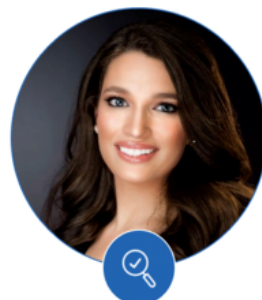
*Credit: Wintana Girma*

**Wintana Girma**

GRC Analyst, Third Party Risk Management, Rush University Medical Center

*NICE Framework Work Roles: Risk Management, Authorizing Official/Designating Representative and Cyber Policy and Strategy Planner*

[Listen to the Interview](#)



**Leeza Garber, Esq.**

Privacy & Cybersecurity Attorney; Co-Founder of Can. Trust. Will., LLC;



**Charles Britt**

Information Systems Security Officer, U.S. Food and Drug



**Santi Kiran**

Security Control Assessor, National Institute for Standards and

The NICE Program Office issues  
to illustrate application of the NICE

and download the transcripts.



COLLECT & OPERATE

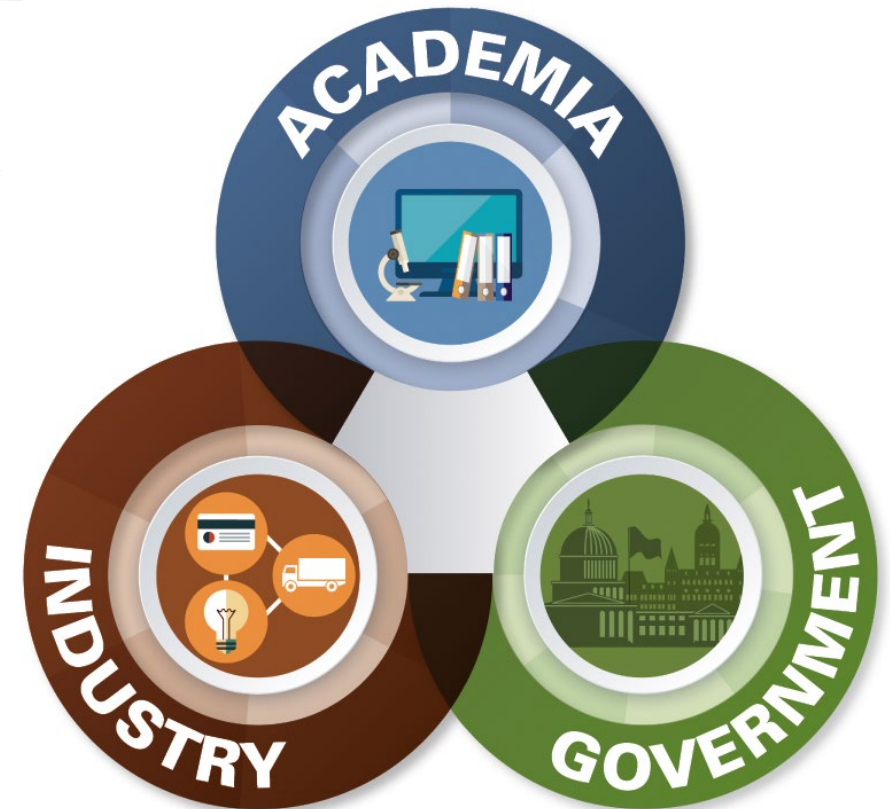


INVESTIGATE

# Stakeholder Engagement

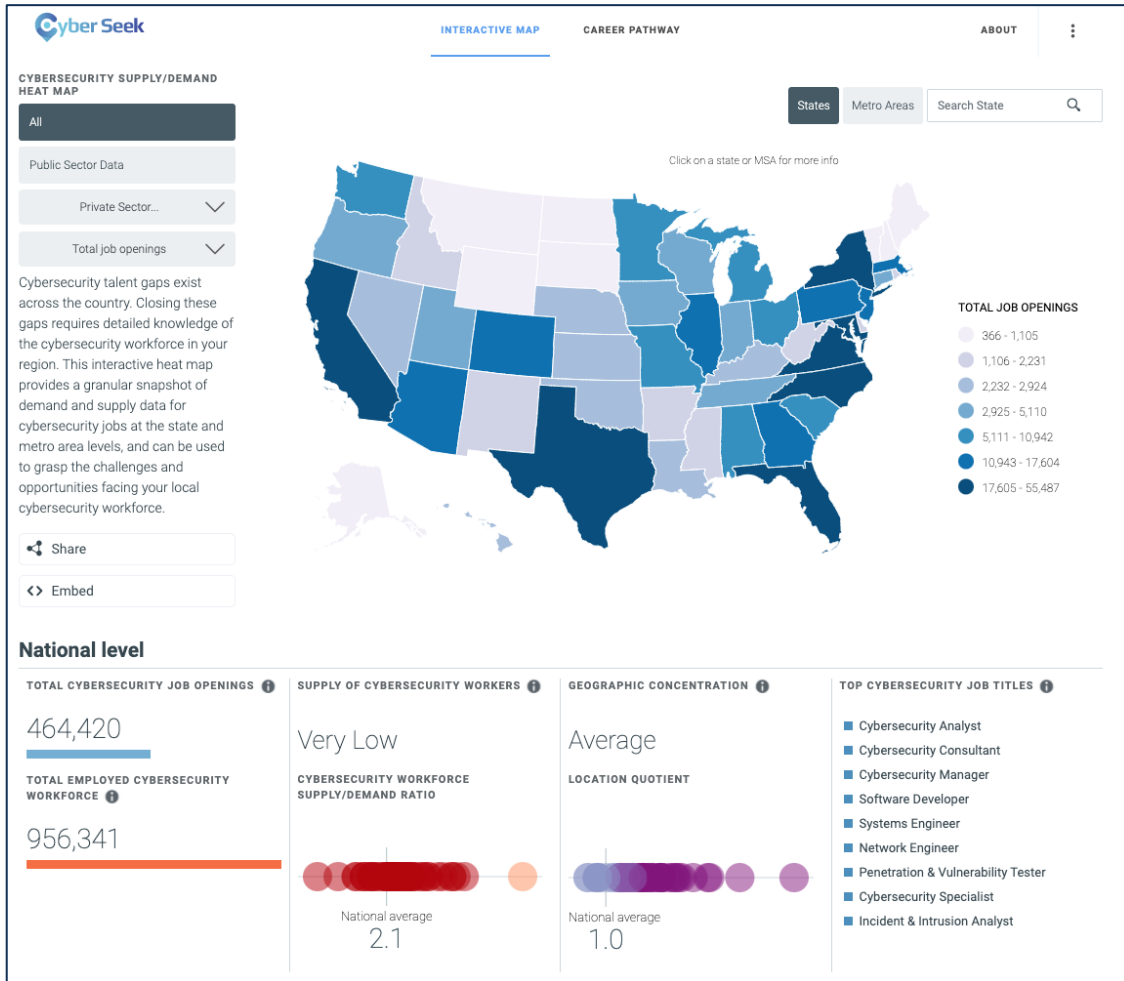
# Consultative Process

- NICE Interagency Coordinating Council
- NICE Community Coordinating Council
- Working Groups
  - Modernize Talent Management
  - Promote Career Discovery
  - Transform Learning Process
- Communities of Interest
  - Apprenticeships in Cybersecurity
  - Cybersecurity Skills Competitions
  - K12 Cybersecurity Education
  - NICE Framework Users



[nist.gov/nice/community](https://nist.gov/nice/community)





[CyberSeek.org](https://www.cyberseek.org)

**Train. Compete. Win.**

US Cyber Games brings together talented cybersecurity athletes, coaches, & industry leaders to build the first US Cyber Team.

[USCyberGames.com](https://www.uscybergames.com)

## SPOTLIGHT ARTICLES



### Cybersecurity Opportunities in the U.S. Air Force

*By Steven Comer, Instructor, 333d Training Squadron, United States Air Force*



### Mentoring Makes the Difference in Cybersecurity

*By Noreen Njoroge, Founder of Cisco's Global Mentoring Program*



### CTE CyberNet: Strengthening Cybersecurity Education

*By Albert Palacios, CTE CyberNet Program Manager, U.S. Department of Education*

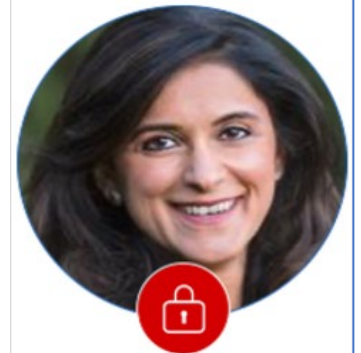
## FRAMEWORK IN FOCUS



**Lonnie Harris**  
Director, Security Enterprise Engineering, Equifax, Inc.



**Carolyn Schmidt**  
Program Manager, Office Of Information Systems Management, National Institute of Standards and Technology



**Anju Chopra**  
Senior Vice President, Cyber Technologies, Kroll

# NICE One Pagers



The image displays a grid of nine NICE One Pagers, each with a distinct color header and content area. The topics are: National Center for Academic Excellence in Cybersecurity, Cyber Ranges, Advanced Technology Education Programs, Cybersecurity Competitions, NICE Cybersecurity Workforce Framework (NIST Special Publication 800-612), RAMPS for Cyber Education and Workforce Development, CyberCorps® Scholarship for Cybersecurity Education and Workforce Development, Cybersecurity Workforce Demand, and Cybersecurity Apprenticeships. Each page includes text, logos of partner organizations, and statistics. The NICE logo is present at the bottom of each page.

[nist.gov/itl/applied-cybersecurity/nice/resources](https://nist.gov/itl/applied-cybersecurity/nice/resources)

## The National Initiative for Cybersecurity Education Cybersecurity Workforce Framework

NIST Special Publication 800-181

### FRAMEWORK

This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development.

### DEVELOPMENT PROCESS

The National Initiative for Cybersecurity Education (NICE) Framework improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

1. Collected and analyzed reference materials (reports, briefings, job task analyses, etc.) from across the government related to workforce contracts. Some of the reviewed resources include: Office of Personnel Management's occupational standards (OPM, 2016), Job descriptions from the Department of Labor's O\*NET database (2015), DoD 8570.01-M Information Assurance Workforce Improvement Program (DoD, 2010), DoD Cyber Workforce Framework, Joint Cybersecurity Training and Education Standards (JCRC), DoD Counterintelligence in Cyberspace Training and Workforce Transformation Working Group Report on Cybersecurity Competencies.
2. Refined existing definitions of cybersecurity specialty areas based on collected information.
3. Conducted focus groups with subject matter experts (SMEs) to identify and define specialty areas not noted in previous versions of the Framework (e.g., Cybersecurity Management and Language Analysis).
4. Conducted focus groups to shape category, specialty area, and work role definitions and align and review tasks and KSAs for each work role.
5. Identified, collected, and wrote new tasks and KSAs, where appropriate.
6. Refined Framework as necessary through workshops, meetings, and stakeholder input (ongoing).

### CYBERSECURITY WORK CATEGORIES

OVERSEER AND GOVERN	OPERATE AND MAINTAIN	INVESTIGATE	COLLECT AND OPERATE	ANALYZE	SECURE PROVISION	PROTECT AND DEFEND
---------------------	----------------------	-------------	---------------------	---------	------------------	--------------------

### WHAT IS THE CYBERSECURITY WORKFORCE?

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

**CATEGORIES:** A high-level grouping of common cybersecurity functions

**SPECIALTY AREAS:** Represent an area of concentrated work, or function, within cybersecurity and related work

**WORK ROLES:** The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role

**TASKS:** Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

**KSAs:** Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

### BUILDING BLOCKS FOR A CAPABLE AND READY CYBERSECURITY WORKFORCE

The NICE Framework provides employers, current and future cybersecurity workers, training and certification providers, education providers, and technology providers with a national standard for organizing the way we define and talk about cybersecurity work, and what is required to do that work.

## National Cybersecurity Career Awareness Week

November 13-18, 2017

National Initiative for Cybersecurity Education (NICE)

### Problem

There is an increasing need for qualified cybersecurity professionals, and a lack of understanding about what a cybersecurity professional does, what jobs are available in cybersecurity, and what cybersecurity career and academic pathways exist.

There are an estimated 295,000 active openings for cybersecurity-related jobs in the United States as of August 2017 (CyberSeek).

Globally, projections suggest a cybersecurity workforce shortage of 1.8 million by 2022 (ISC<sup>2</sup>).

Cybersecurity Awareness ≠ Cybersecurity Career Awareness

### About

The National Cybersecurity Career Awareness Week, brought to you by the National Initiative for Cybersecurity Education (NICE), is a week-long celebration focused on increasing awareness about careers in cybersecurity and how building a national cybersecurity workforce enhances America's security and economic prosperity.

NICE brings to the forefront information of local, regional, and national interest to inspire, educate and engage citizens to pique their interest in cybersecurity careers.

National Cybersecurity Career Awareness Week takes place during November's National Career Development Month, and each day of the week-long celebration provides an opportunity to learn about the contributions, innovations, and opportunities that can be found by choosing a career in cybersecurity.

### Objectives

- Create excitement around increasing public awareness and engagement in building a strong cybersecurity workforce.
- Emphasize the demand and opportunities in the field of cybersecurity.
- Increase awareness around the multiple career options within the field of cybersecurity.
- Highlight the numerous pathways to enter the cybersecurity career field.
- Showcase programs that increase participation of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce.
- Advance the NICE Strategic Plan objective to inspire cybersecurity career awareness with students.

### Activities

Day 1: Nov. 13, 2017 – Kickoff Event at the National Cybersecurity Center of Excellence

Day 2: Nov. 14, 2017 – Increasing underrepresented populations

Day 3: Nov. 15, 2017 – Webinar: Nontraditional Pathways of Apprenticeship and Cooperative Education

Day 4: Nov. 16, 2017 – Infusing Cybersecurity Across the Education Pipeline

Day 5: Nov. 17, 2017 – Identifying Academic and Career Pathways

Day 6: Nov. 18, 2017 – Increase Career Awareness through Informal Activities. Ending session at the National Cryptologic Museum.

The 2017 activities have been organized around the four prongs of the 4-12 Cybersecurity Education Implementation Plan; however, an encouragement of stakeholders to engage in the week-long celebration.

### References

1. [CyberSeek: The National Cybersecurity Workforce Shortage](#)
2. [ISC<sup>2</sup> Global Cybersecurity Workforce Shortage Report](#)
3. [NICE Strategic Plan](#)

- **Cybersecurity Career Awareness Week**

- October 18-23, 2021
- October 17-22, 2022

- **NICE Webinars**

- Digital Citizenship: October 20, 2021 at 2-3pm ET
- NICE Framework: December 15, 2021 at 2-3pm ET

- **Federal Cybersecurity Workforce Summit**

- Webinar on Apprenticeships: October 26, 2021 at 1:30-3pm ET
- Webinar on Diversity, Equity, Inclusion, and Accessibility: January 25, 2021 at 1:30-3pm ET
- Annual Summit: April 26, 2022

- **Annual NICE Conference & Expo**

- NICE Symposium: A Coordinated Approach to Supply Chain Risks: November 16, 2021 at 1-5pm ET
- Annual Conference: June 6-8, 2022

- **NICE K12 Cybersecurity Education Conference**

- Annual Conference: December 6-7, 2021

- **FISSEA: Federal Information Security Educators**

- Winter Forum: February 15, 2022
- Annual Conference: May 18-19, 2022



# STAY IN TOUCH

---

## CONTACT US



[NIST.gov/NICE](https://www.nist.gov/NICE)



[LinkedIn.com/company/NIST-NICE](https://www.linkedin.com/company/NIST-NICE)



[@nist](#)



[@nistcyber](#)