

The NICE Framework:

Preparing a Job-Ready Cybersecurity Workforce

NIST SP 800-181r1

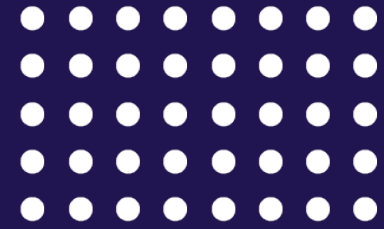
Karen A. Wetzel, Manager of the NICE Framework

karen.wetzel@nist.gov

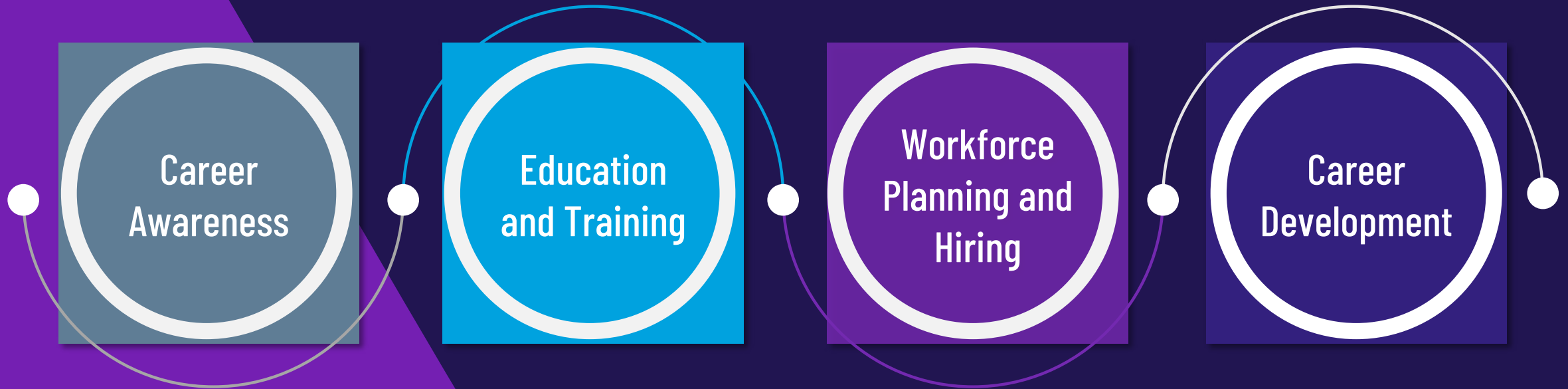
Today's Agenda

- Today's Cybersecurity Workforce
- What is a Workforce Framework?
- NICE Workforce Framework for Cybersecurity
- Using the NICE Framework to Address Challenges





NICE Focus Areas



NICE Strategic Plan and Implementation Plan (2021-2025)



Promote the Discovery of Cybersecurity Careers and Multiple Pathways



Transform Learning to Build and Sustain a Diverse and Skilled Workforce



Modernize the Talent Management Process to Address Cybersecurity Skills Gaps



Expand Use of the Workforce Framework for Cybersecurity (NICE Framework)



Drive Research on Effective Practices for Cybersecurity Workforce Development

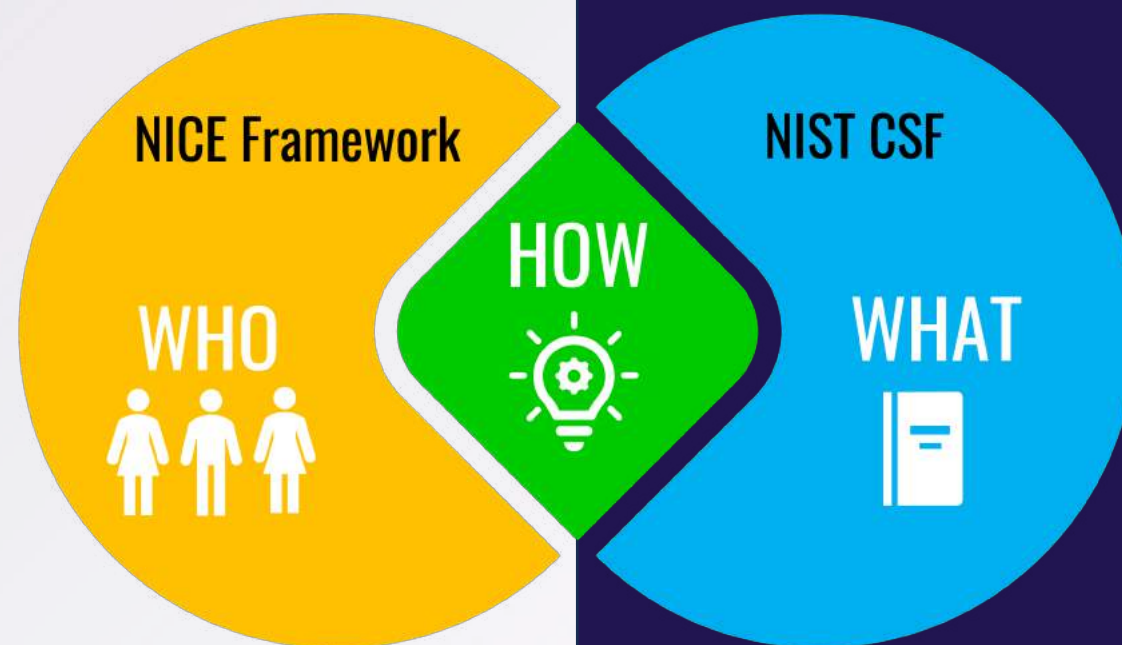
NICE Framework Focus: Who and How

NIST Cybersecurity Framework (CSF):
Standards, guidelines and best practices
to manage cybersecurity risk

www.nist.gov/cyberframework

NICE Framework:
Education, Training, and Workforce

Where They Connect: How



Cybersecurity Workforce Challenges

- Aging workforce
- Growing demand
- Low retention
- Low availability of entry points for new workers
- Low diversity
- Highly experienced and skilled workforce requirements





Cybersecurity Workforce Opportunities

- Demand for workers is high
- Work is well paying
- Mission is attractive
- Positions can often accommodate remote work
- Multiple career pathways

A Playbook for Workforce Frameworks

<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/playbook-workforce-frameworks>

The screenshot shows the NIST website interface. At the top, it says "An official website of the United States government" and "Here's how you know". The NIST logo is on the left, and a search bar and "Menu" button are on the right. Below the header, it says "Applied Cybersecurity Division / National Initiative for Cybersecurity Education (NICE)". The main heading is "NICE FRAMEWORK RESOURCE CENTER". On the left is a navigation menu with sections: "About", "Current Version", "Resources" (with sub-items: Users Group, Employer Resources, Education and Training, Provider Resources, Learner Resources, Success Stories, Framework in Focus, Presentations, and "Playbook for Workforce Frameworks" which is highlighted), "Related Programs", and "NICE Homepage". A "CONNECT WITH US" button with social media icons is at the bottom left. The main content area is titled "Playbook for Workforce Frameworks". It includes an introductory paragraph, a list of core principles, a list of bullet points, and a section titled "BENEFITS OF A MODEL WORKFORCE FRAMEWORK" with another introductory paragraph and a list of bullet points.

Playbook for Workforce Frameworks

The Playbook for Workforce Frameworks is instrumental in supporting a standard approach to developing workforce frameworks to enable interoperability and improve communication, innovation, and mobility across workforces.

The playbook defines a model workforce framework built on the principles of agility, flexibility, modularity, and interoperability. Its core principles include:

- The concepts of work and learner are described in terms that can be applied to any organization.
- A modular, building-blocks approach based on Task, Knowledge, and Skill (TKS) statements recognizes that all organizations execute common tasks and context-unique tasks that require knowledge and skills to complete.
- TKS statements can be used to define Competency Areas, establish Work Roles, and build teams that reflect an organization's own unique context and needs.

The playbook details the model framework's components, including the TKS statement building blocks and their applications as Work Roles and Competency Areas, and provides developers with resources on how to develop these components and describe common uses with their community. The playbook is intended to be a living document, with additional resources being developed to add to it over time.

BENEFITS OF A MODEL WORKFORCE FRAMEWORK

By describing information about a defined area of work, a workforce framework provides a common language that can improve communication and align stakeholders' expectations. For example:

- **Employers** can use a workforce framework to conduct workforce assessments and identify gaps, improve recruitment and retention efforts, manage employee performance, and establish strategic workforce development initiatives.

Benefits of a Workforce Framework
Workforce Framework Uses
Workforce Framework Components
Supporting Resources

Workforce Frameworks: Example Uses

- Promote cybersecurity career awareness in K12 and beyond
- Create curriculum to prepare an effective workforce and highlight connection to jobs
- Assess current cybersecurity workforce and prepare for future needs
- Identify job requirements, write job descriptions, and assess candidates
- Support continuous learning, career pathways, and career development



Workforce Framework Attributes

Agility

People, processes, and technology mature and must adapt to change. A workforce framework enables organizations to keep pace with a constantly evolving ecosystem.



Flexibility

There is no one-size-fits-all solution to common challenges. A workforce framework enables organizations to account for their unique operating context.

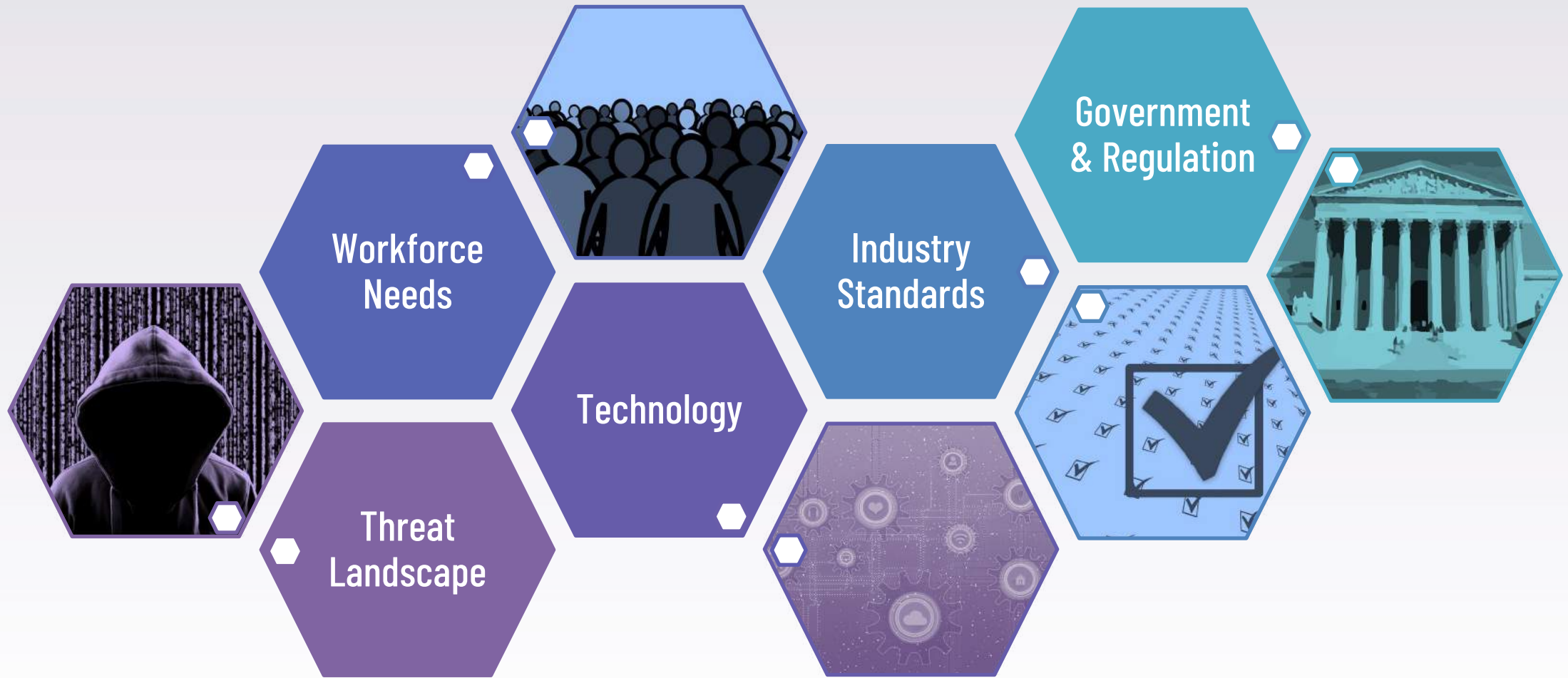
Interoperability

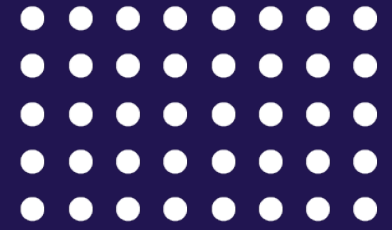
Solutions to common challenges may be unique, but they must agree upon consistent use of terms. A workforce framework enables organizations to exchange workforce information using a common language.

Modularity

In addition to cybersecurity, organizations manage other risks within the enterprise. A workforce framework enables communication about these other workforces within the enterprise and across sectors.

Adapting the Framework: Local Factors





The NICE Framework

Workforce Framework for Cybersecurity (NICE Framework)

A common, consistent vocabulary to **clearly share information** about what a workforce needs to know

A modular, building-blocks approach based on **Task, Knowledge, and Skill (TKS) statements**

The concepts of work and learner can be applied **to any organization**

Enables the establishment of **regular processes**

For use in **career awareness, education and training, hiring and career development, & workforce planning and assessment**

**NIST Special Publication 800-181
Revision 1**

**Workforce Framework
for Cybersecurity
(NICE Framework)**

Rodney Petersen
Danielle Santos
Matthew C. Smith
Kiren A. Wenzel
Greg Witt

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.SP.800-181r1>

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

**Reference Spreadsheet
for the
Workforce Framework
for Cybersecurity
(NICE Framework)**

NIST Special Publication 800-181, Revision 1
www.nist.gov/nice/framework

NOTE TO READERS:
NIST Special Publication 800-181, Revision 1 was published November 26, 2020. This revision presents a streamlined set of "building blocks" comprised of Work Roles, Knowledge, and Skills (TKS). These building blocks and corresponding Work Roles and Competencies will be maintained as separate artifacts and will be subject to ongoing review and updates with a defined change process and indication of version control to manage and communicate changes.
Until these updates occur, the 2017 NICE Framework sections of Work Role, Tasks, and Knowledge and Skill statements found in this reference spreadsheet remain to be valid.

Work Role ID	KSAs	Tasks
SP-RSK-001	Click to view KSAs	Click to view Tasks
SP-RSK-002	Click to view KSAs	Click to view Tasks
SP-DEV-001	Click to view KSAs	Click to view Tasks
SP-DEV-002	Click to view KSAs	Click to view Tasks
SP-ARC-001	Click to view KSAs	Click to view Tasks

Table of Contents: SP-RSK-001 KSAs | SP-RSK-001 Tasks | SP-RSK-002 KSAs | SP-RSK-002 Tasks | SP-DEV-001 KSAs | SP-DEV-001 Tasks | SP-DEV-002 KSAs

Who is the NICE Framework For?

- Track workforce capabilities
- Create job descriptions
- Develop employees
- Provide career pathways

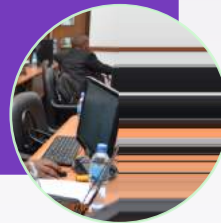
EMPLOYERS



- Learn about the variety of cybersecurity work roles
- Develop knowledge and skills in a defined area of expertise
- Apply learning and demonstrate capability

LEARNERS

students, job-seekers, and employees



- Develop learning courses and programs
- Align teaching with the NICE Framework
- Conduct performance-based assessments

EDUCATION, TRAINING, AND CREDENTIAL PROVIDERS



GOVERNMENT • INDUSTRY • ACADEMIA

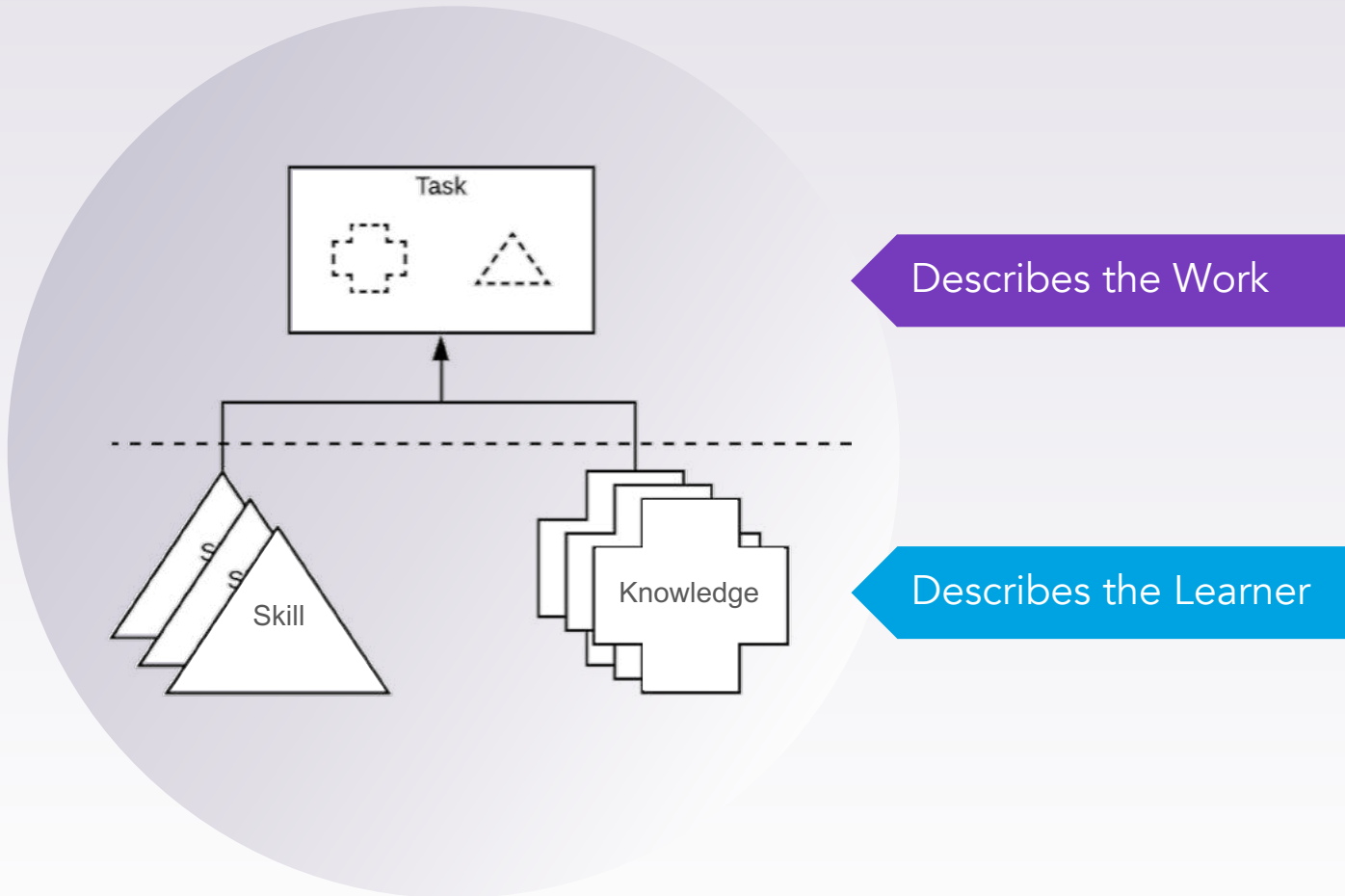


NICE Framework Components

TKS Statements,
Work Roles, and Competency Areas



NICE Framework Building Blocks: Task, Knowledge, and Skill (TKS) Statements



TKS Definitions

- **Task:** An activity that is directed toward the achievement of organizational objectives.
- **Knowledge:** A retrievable set of concepts within memory.
- **Skill:** The capacity to perform an observable action.

Using the NICE Framework: Building Block Applications



WORK ROLES

- Groupings of Task statements
- Work an individual or team is responsible for



COMPETENCY AREAS

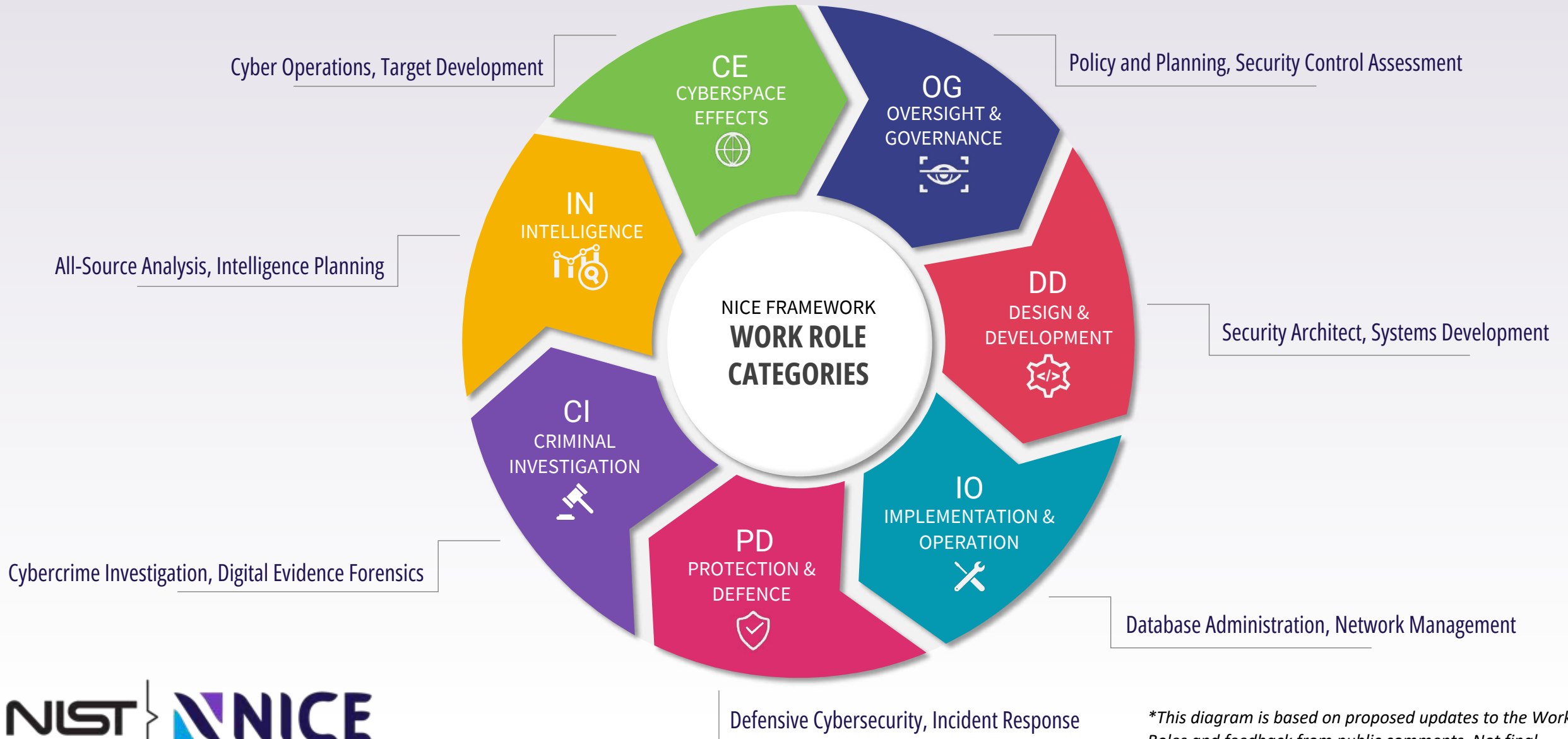
- Groupings of related Knowledge and Skill statements
- Correlate with capability to perform Tasks in a domain



TEAMS

- Created Using Competency Areas or Work Roles

NICE Framework Work Role Categories and example roles*



*This diagram is based on proposed updates to the Work Roles and feedback from public comments. Not final.

Occupations, Jobs, and Work Roles

Work Role:

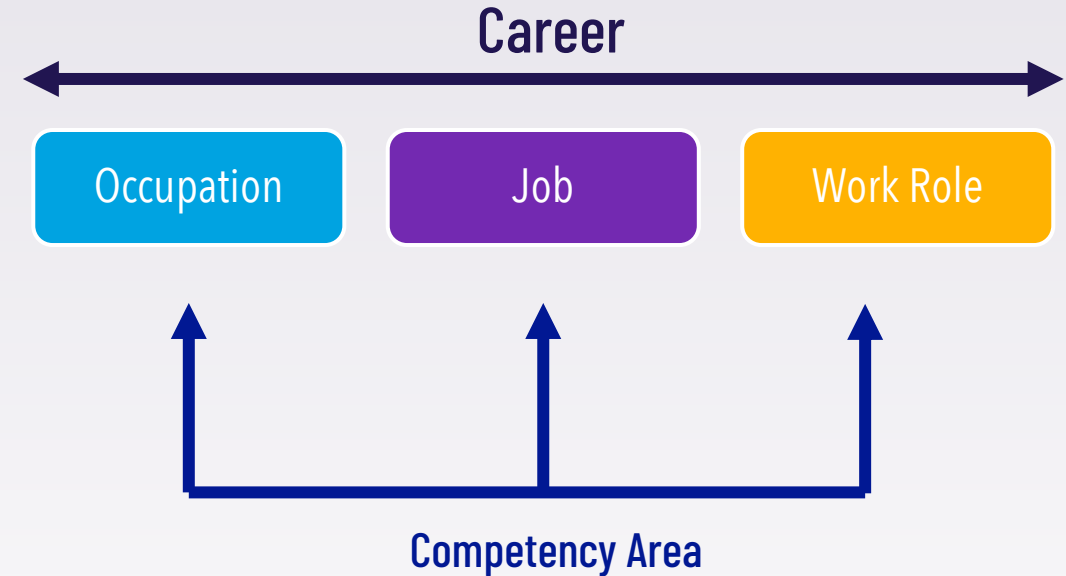
A grouping of work for which someone is responsible or accountable

Work Roles:

- Are not synonymous with job titles or occupations
- May apply to many varying job titles
- Can be combined to create a particular job

Consist of:

- Tasks that constitute the work to be done



NICE Framework

Work Role Examples

Incident Response Category: Protection and Defense	Systems Management Category: Oversight and Governance	Threat Analysis Category: Protection and Defense
Responsible for investigating, analyzing, and responding to network cybersecurity incidents.	Responsible for the cybersecurity of a program, organization, system, or enclave.	Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat and warning assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.
<ul style="list-style-type: none"> ● 17 Tasks ● 40 Knowledge/Skill/Ability 	<ul style="list-style-type: none"> ● 53 Tasks ● 59 Knowledge/Skill/Ability 	<ul style="list-style-type: none"> ● 29 Tasks ● 32 Knowledge/Skill/Ability

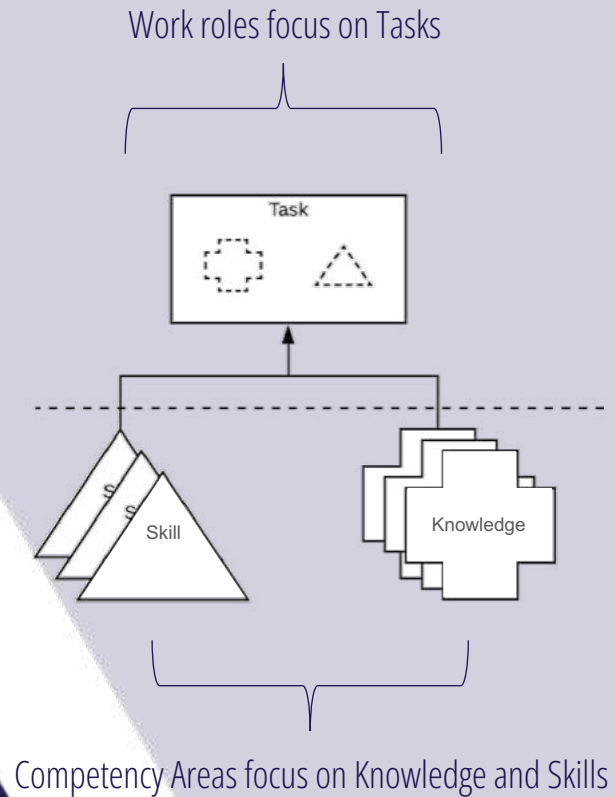
Example Tasks (Systems Management)

T0213	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.
T0219	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.
T0254	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
T0263	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.

NICE Framework Competency Areas

Clusters of related Knowledge and Skill statements that correlate with one's capability to perform Tasks in a particular domain.

Competency Areas can help learners discover areas of interest, inform career planning and development, identify gaps for knowledge and skills development, and provide a means of assessing or demonstrating a learner's capabilities in the domain.



- ❑ **Name:** Clearly signals the area that will be described.
- ❑ **Description:** Provides simple and clear language that focuses on the learner
- ❑ **Associated TKS Statements**

NICE Framework Competency Areas: Preparing a Job-Ready Workforce



- Competency Areas and the NICE Framework
- Competency Area Development
- Example Uses

The screenshot shows the NIST CSRC website interface. At the top, there's a search bar and a menu icon. Below that, the header identifies the site as the 'COMPUTER SECURITY RESOURCE CENTER'. A 'PUBLICATIONS' tab is active, displaying the title 'NISTIR 8355' and 'NICE Framework Competency Areas: Preparing a Job-Ready Workforce'. The page includes a 'Date Published' of June 2023, a 'Planning Note' with a call to action for comments, and the author 'Karen Wetzel (NIST)'. An 'Abstract' section provides a detailed overview of the framework's purpose and structure. A 'Keywords' section lists terms like 'competency', 'cybersecurity', and 'workforce'. A 'Control Families' section at the bottom indicates 'None selected'. On the right side, there are sections for 'DOCUMENTATION' (including links to the publication and supplemental materials) and 'TOPICS' (listing 'Security and Privacy' and 'Applications').

The cover page features the NIST logo at the top left and the title 'NIST Internal Report NIST IR 8355' at the top right. The main title is 'NICE Framework Competency Areas' with the subtitle 'Preparing a Job-Ready Cybersecurity Workforce'. The author's name, 'Karen A. Wetzel', is listed below the subtitle. A note at the bottom states that the publication is available free of charge from a DOI link. The NIST logo and full name are at the bottom right.

<https://csrc.nist.gov/publications/detail/nistir/8355/final>

NICE Framework Competency Areas May...

- Be **additive** to one or more Work Roles
- Be used **independently** of Work Roles
- Represent domains that **span** multiple Work Roles
- Represent **emerging** domains that do not yet have established Work Roles

In addition, Competency Areas:
Do not duplicate existing Work Roles



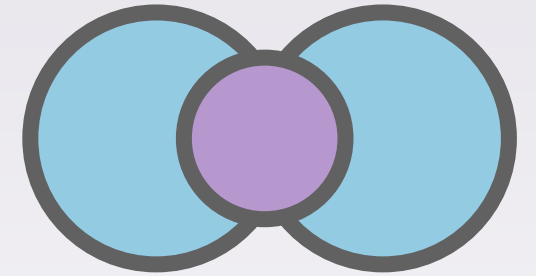
Proposed NICE Framework Competency Areas

15 Competency Areas, representing:
Fundamental Areas • Emerging Areas • Unique Domains

1. Access Controls
2. AI Security
3. Asset Management
4. Cloud Security
5. Communications Security
6. Cryptography
7. Cybersecurity Fundamentals
8. Cybersecurity Leadership
9. Data Security
10. DevSecOps
11. Cyber Resiliency
12. OS Security
13. OT Security
14. Secure Programming
15. Supply Chain Security

Applying Competency Areas: Additive to Work Role(s)

- When additional capabilities are necessary for a particular Work Role at your organization, the Competency Area can be added to supplement that role
- A position responsible for more than one Work Role may need the Competency Area across the multiple roles
- An organization may want a candidate to demonstrate capability in a defined Competency Area for particular Work Roles

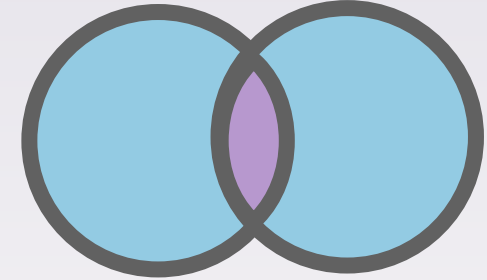


Example:

Cloud Security Competency Area + Security Architecture Work Role

Applying Competency Areas: Span Multiple Work Roles

- To improve communication and coordination in a specific sector or domain
- For staff who don't work in cybersecurity but need cybersecurity expertise to mitigate risks
- A starting place to shift into cybersecurity



Example:

OT Cybersecurity Competency Area *needed by:*

- Facilities Managers
- Information Systems Security Developers

Applying Competency Areas: Independent, Emerging Domains

- A starting place for learning about cybersecurity work
- A way to shift to a different or related area of cybersecurity
- A way to develop higher-level expertise in an area
- A way to represent emerging domains prior to Work Role consensus



Examples:

- Cybersecurity Fundamentals
- Secure Programming
- AI Cybersecurity

Competency Areas Authoring Guide

- What are Competency Areas?
- Competency Areas and Work Roles
- How to Draft Competency Areas

Benefits of a Workforce Framework
Workforce Framework Uses
Workforce Framework Components
Supporting Resources

The screenshot shows the NIST website's 'NICE Framework Resource Center' page. The main heading is 'Playbook for Workforce Frameworks'. The page includes a sidebar with navigation links such as 'About', 'Current Version', 'Resources' (with sub-links for Users Group, Employer Resources, Education and Training, Provider Resources, Learner Resources, Success Stories, Framework in Focus, and Presentations), 'Playbook for Workforce Frameworks', 'Related Programs', and 'NICE Homepage'. The main content area provides an overview of the playbook's purpose and lists key principles and components. A 'CONNECT WITH US' section at the bottom left features icons for email, LinkedIn, and Twitter. The footer includes the NIST logo and the text 'NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE'.

The cover page features the title 'Competency Areas Authoring Guide for Workforce Frameworks' at the top. Below the title, it indicates the document is a 'Working Draft' dated 'June 21, 2023'. At the bottom right, the NIST logo is displayed alongside the text 'NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE'.

<https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/playbook-workforce>

Measuring Cybersecurity Workforce Capabilities: Defining a Proficiency Scale for the NICE Framework

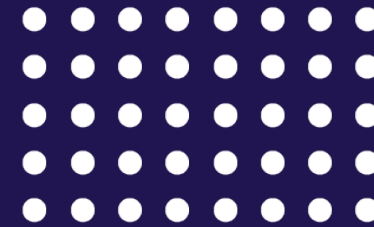
Key Characteristics of Workplace Proficiency Scales

- **Demonstrative:** How capability is evidenced
- **Supervision:** Amount and type for the level
- **Professional Skills:** Soft skills, employability skills...



Recommendations

1. Establish a **workplace-focused NICE Framework proficiency scale** to be applied to Competency Areas and Work Roles
2. Encourage the NICE Modernize Talent Management Working Group to establish a Project Team for NICE **Strategic Plan Goal #3: Align qualification requirements according to proficiency levels**
3. Engage stakeholders and subject matter experts to **develop statements of proficiency** to apply to NICE Framework



Example Use: Hiring

Common Challenges

Unclear workforce needs

Working without a detailed position description

Conducting a candidate search with unrealistic goals






Do we have the right people
on our cybersecurity team?

Solution: Conduct a workforce assessment using the NICE Framework


- Determine needed Work Roles
- Assess current cybersecurity staff in needed Competency areas
- Identify gaps and provide requisite training



How can we be sure to hire the right candidate?

Solution: Use the NICE Framework to...

- Identify Competencies & Work Roles the new hire will be responsible for
- Use language from the NICE Framework in your job description
- Assess candidates for needed knowledge and skills

A black silhouette of a person standing on the left side of the slide, facing right. A dark blue speech bubble points from the person's mouth area towards the center of the slide. The speech bubble contains white text.

I'm looking to shift to a new cybersecurity role in my organization but want to make sure I'm prepared.

Solution: Upskill and reskill with the NICE Framework

- Use related Work Roles in career pathing
- Clearly communicate organizational needs
- Identify areas of strength and weakness – and then focus on areas that need work

IT Cybersecurity Specialist

Typical work assignments include:

- Ensures that the implemented security **safeguards** are adequate to assure the **integrity, availability and confidentiality** of the information being processed, transmitted or stored consistent with the level of sensitivity of that information.
- **Plans the work** to be accomplished by subordinate civilian and contractor; sets and adjust short-term priorities, and prepare schedules for completion of work; assigns work to subordinates based on priorities, selective consideration of the difficulty, requirements of assignments, and the capabilities of employees
- Perform real-time **cyber defense incident handling** (e.g., **forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation**) tasks to support deployable Incident Response Teams.
- Analyzes **policy** and recommends improvements.
- Serves as an expert consultant evaluation for functional teams, to assist them in **anticipating, identifying, evaluating, mitigating and minimizing risks associated with IT systems vulnerabilities.**

Example Job Description

Additional Resources

www.nist.gov/nice/framework

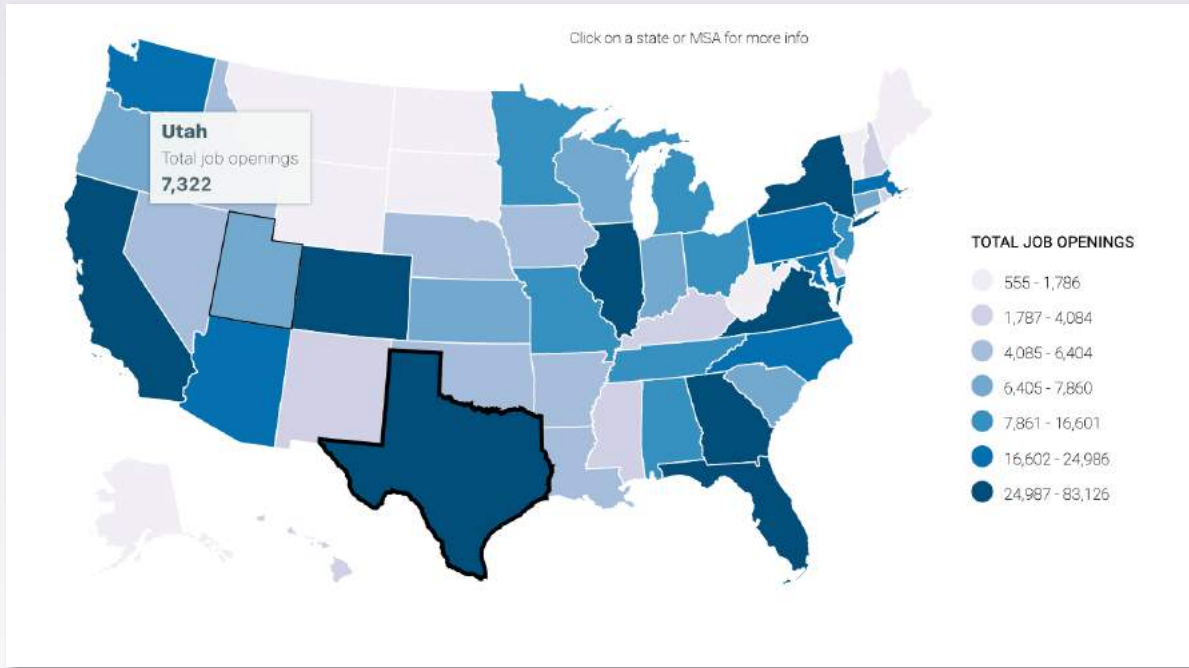


NICE Framework Resource Center

- Getting Started & FAQ
- Documents & Data
- Translations
- Playbook for Workforce Frameworks
- Success Stories (Case Studies) and Framework in Focus (Practitioner Interviews)
- Resources for Employers, Education & Training Providers, and Learners
- Coming Soon: Employers Guide to Developing Job Descriptions
- Planned: Usage Guides, Job Profiles, Career Pathways, Proficiency Levels

NICE Framework Tools

- [CyberSeek](#): An interactive cybersecurity jobs heat map across the U.S. by state and metropolitan areas and career pathway tool.
- [NICE Framework Tool & Keyword Search](#): Enables browsing and searching.
- [NICE Framework Mapping Tool](#): Answer questions about your federal cybersecurity-related position and the tool will show you how it aligns to the NICE Framework and what can be done to strengthen your cybersecurity team.
- [NICCS Education and Training Catalog](#): Cybersecurity professionals across the nation can find over 6,000 cybersecurity-related courses aligned with the NICE Framework.
- [NICCS Cyber Career Pathways Tool](#): Includes common relationships between roles as well as frequently used titles in each role. (Federal)
- [NICE Challenge Project](#): Real-world cybersecurity challenges within virtualized business environments to provide students with workforce experience before entering the workforce.



Texas

TOTAL CYBERSECURITY JOB OPENINGS

83,126

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

104,791

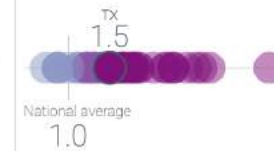
SUPPLY/DEMAND RATIO



GEOGRAPHIC CONCENTRATION

High

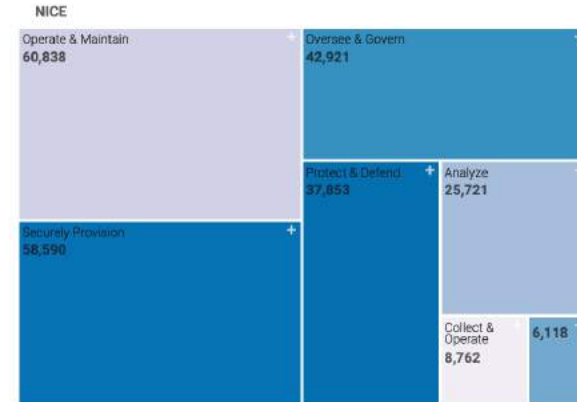
LOCATION QUOTIENT



TOP CYBERSECURITY JOB TITLES

- Cybersecurity Analyst
- Penetration & Vulnerability Tester
- Software Developer
- Cybersecurity Consultant
- Cybersecurity Manager
- Network Engineer
- Systems Engineer
- Senior Software Developer
- IT Director

JOB OPENINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY

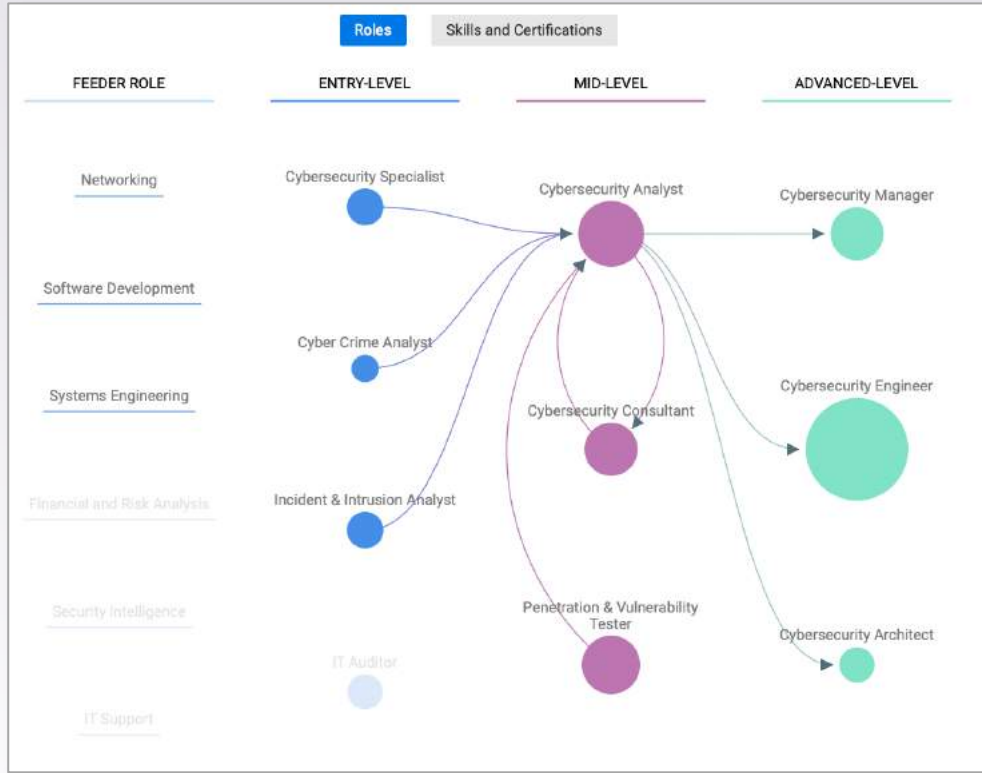


Notes: The NICE Workforce Categories are not mutually exclusive- one job could perform multiple roles within the framework. The data shown here are not intended to be aggregated.

CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION



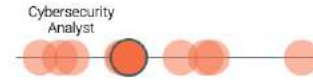
Cyber Seek Cybersecurity Career Pathway: Cybersecurity Analyst



Cybersecurity Analyst

AVERAGE SALARY

\$107,517



COMMON JOB TITLES

- Cybersecurity Analysts
- Information Security Analysts
- Security Analysts
- IT Security Analysts
- Cyber Threat Analysts

REQUESTED EDUCATION (%)



TOTAL JOB OPENINGS

27,091



TOP FUTURE SKILLS REQUESTED

Skills	5-Year Projected Growth
Public Cloud Security	121%
Comprehensive Software Security	114%
Threat Hunting	105%
Security Information and Event Management (SIEM)	65%
Threat Intelligence & Response	53%

COMMON NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORIES

- Securely Provision
- Operate and Maintain
- Protect and Defend
- Analyze
- Investigate
- Oversee and Govern
- Collect and Operate

TOP CERTIFICATIONS REQUESTED

- Certified Information Systems Security Professional
- GIAC Certifications
- CompTIA Security+
- Certified Information System Auditor (CISA)
- Certified Information Security Manager

TOP SKILLS REQUESTED

- 1 Cyber Security
- 2 Computer Science
- 3 Vulnerability
- 4 Auditing
- 5 Incident Response
- 6 Risk Analysis
- 7 Firewall
- 8 Risk Management
- 9 Cyber Threat Intelligence

NICCS Pathways Tool: Cyber Defense Analyst

Details

Tasks

KSAs

Capability Indicators

Common Relationships

Federal Data

Cyber Defense Analyst

Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Community: Cybersecurity
Category: Protect and Defend
Specialty Area: Cyber Defense Analysis
OPM ID: 511

[See USAJOBS listings coded for Cyber Defense Analyst](#)

Related Functional Titles

The following job titles have been identified by subject matter experts as either alternative titles for this work role or including the functions of this work role as part of their job duties.

- Computer Network Defense (CND) Analyst
- Cybersecurity / Information Security Analyst
- Enterprise Network Defense (END) Analyst
- Incident Analyst

Relationship filters:

Selected KSATs

All Federal Core

Compared KSATs

All Federal Core

KSATs

On Ramps

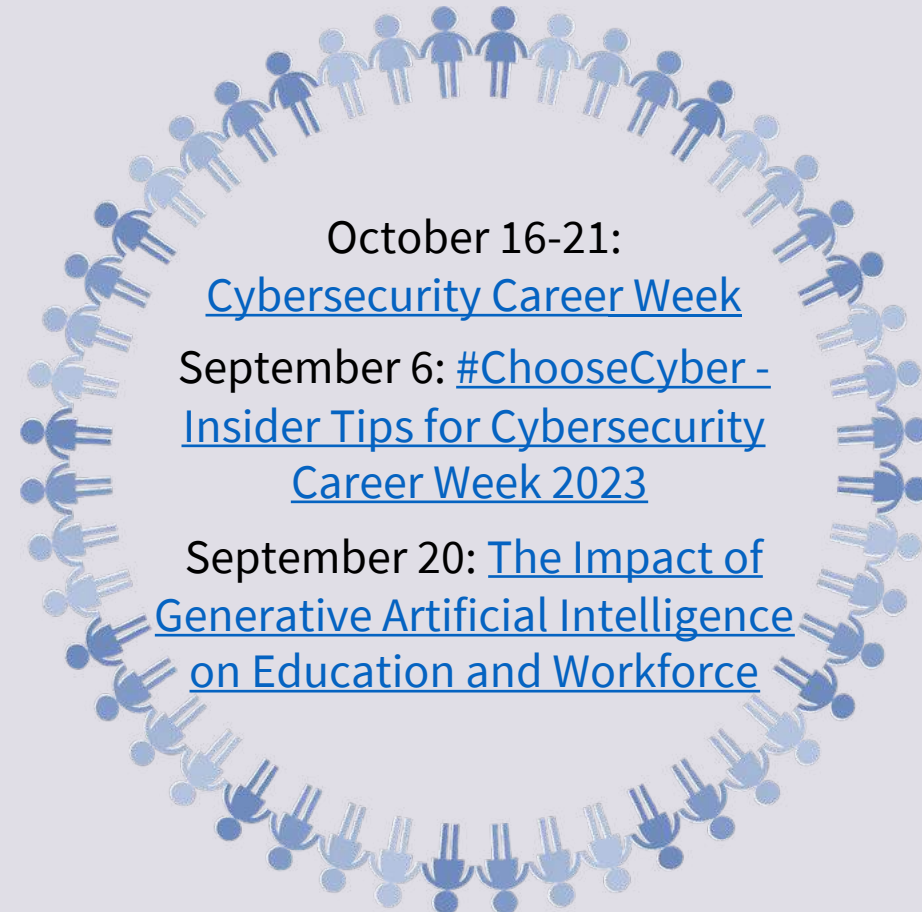
Off Ramps

Secondary Work Roles

[Clear selection](#)

Engage with NICE

- NICE Framework Users Group
 - Sharing and learning how to apply and use the NICE Framework
- NICE Interagency Coordinating Council
 - Open to all federal employees with responsibilities to grow and sustain the Nation's cybersecurity workforce
 - Monthly meetings (next call: July 13, 2023)
- NICE Community Coordinating Council
 - Public and private sector participants
 - Monthly meetings (next call: May 24, 2023)
- Calls for Comments, Workshops, Webinars, Conferences



Questions?

- www.nist.gov/nice/framework
- NICEframework@nist.gov
- karen.wetzel@nist.gov