NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The U.S. National Initiative for Cybersecurity Education (NICE)

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

QUICK FACTS

- Led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce
- A partnership between government, academia, and the private sector

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Mission

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

History

1998: The Comprehensive National Cybersecurity Initiative (CNCI) created. Initiative 8 aims at better preparing the Federal cybersecurity workforce.

2009: Initiative 8 scope expands to include private sector workforce.

2010: Initiative #8, "Expand cyber education," becomes public.

2014: Cybersecurity Enhancement Act of 2014 Title IV establishes the "National cybersecurity awareness and education program" (NICE).

What NICE Does

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Strategic Plan and Implementation Plan
(2021-2025)

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

www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

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
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

CAREER DISCOVERY
Promote the Discovery of Cybersecurity Careers and Multiple Pathways

- Identify and share effective practices for promoting cybersecurity career awareness and discovery
- Increase understanding of multiple learning pathways and credentials that lead to careers identified in the NICE Framework
- Develop and utilize proven tools and resources to identify individuals most likely to succeed in a cybersecurity career
- Provide information and tools about cybersecurity-related career options to those who influence career choices
- Galvanize employers to promote discovery and exploration of cybersecurity career opportunities and work-based learning experiences

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

LEARNING PROCESS
Transform Learning to Build and Sustain a Diverse and Skilled Workforce

- Foster proven learning methods and experiences shown to effectively build and sustain a diverse, inclusive, and skilled cybersecurity workforce
- Advocate for multidisciplinary approaches that integrate cybersecurity across varied curricula that support diverse learners from a variety of backgrounds and experiences
- 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
- Champion the development and recognition of teachers, faculty, and instructors as part of the in-demand workforce

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

TALENT MANAGEMENT
Modernize the Talent Management Process to Address Cybersecurity Skills Gaps

- Enhance the capabilities to effectively recruit, hire, develop, and retain cybersecurity talent
- Utilize new technologies aches to increase connections and fit between employers and job seekers
- Align qualification requirements according to proficiency levels to reflect the competencies and capabilities required to perform tasks in the NICE Framework
- Promote the establishment of more entry-level positions and opportunities that provide avenues for growth and advancement
- Encourage and enable ongoing development and training of employees to foster and keep current talent with diverse skills and experiences
- Nurture effective practices in reskilling the unemployed, underemployed, incumbent workforce, and transitioning veterans to prepare them for careers in cybersecurity

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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

- Document and disseminate methods, resources, and tools shown to successfully expand use of the NICE Framework
- Align the NICE Framework with other cybersecurity, privacy, and risk management publications
- Establish processes for regularly reviewing, improving, and updating the NICE Framework
- Explore development of new tools or integration into existing tools
- Identify and highlight components of the NICE Framework statements that could be potentially performed via automated techniques
- Expand international outreach to promote the NICE Framework

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

RESEARCH
Drive Research on Effective Practices for Cybersecurity Workforce Development

- Research and disseminate results on factors that influence the impact of cybersecurity education, training, and workforce development
- Inspire bold investigation of critical societal and global issues impacting cybersecurity education and workforce, synthesizing data-driven evidence, and providing trustworthy advice
- Prioritize research on the most effective and proven practices for blending successful learning practices across education, training, and workforce development settings
- Utilize research results to inform programs and curriculum design, foster continuous learning opportunities, impact learner success, and ensure

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

The Cybersecurity Workforce Landscape

CyberSeek

CYBERSECURITY SUPPLY/DEMAND HEAT MAP

All

Public Sector Data

Private Sector...

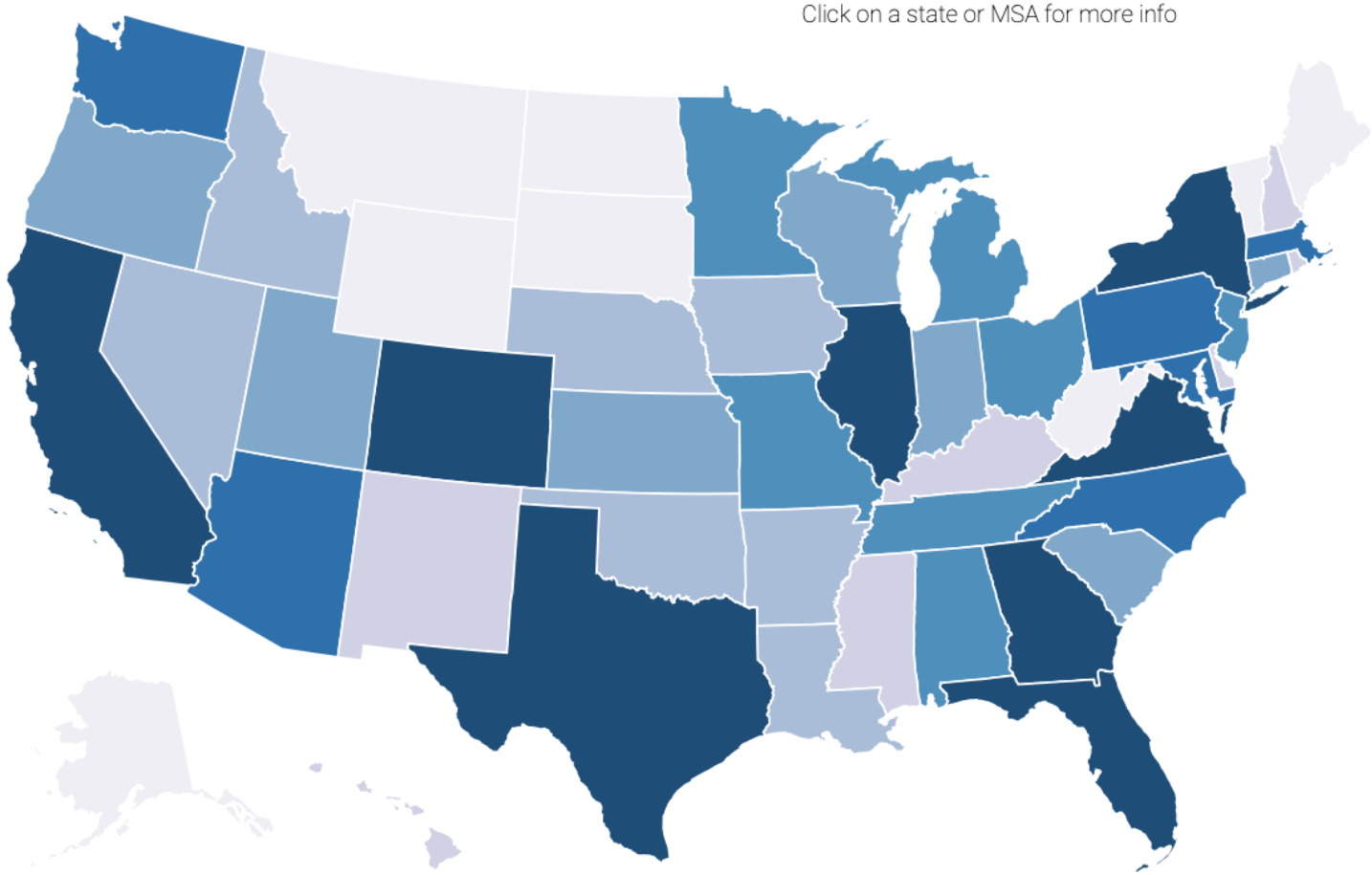
Total job openings

Cybersecurity talent gaps exist across the country. Closing these gaps requires detailed knowledge of the cybersecurity workforce in your region. This interactive heat map provides a granular snapshot of demand and supply data for cybersecurity jobs at the state and metro area levels, and can be used to grasp the challenges and opportunities facing your local cybersecurity workforce.

Share

States | Metro Areas | Search State

Click on a state or MSA for more info



TOTAL JOB OPENINGS

- 555 - 1,786
- 1,787 - 4,084
- 4,085 - 6,404
- 6,405 - 7,860
- 7,861 - 16,601
- 16,602 - 24,986
- 24,987 - 83,126

"Cybersecurity Hiring Momentum Ramps Up"

May 2021 – April 2022

714,548: Cybersecurity Job Openings

1,091,575: Cybersecurity Workers Employed

66%: Nationwide Supply/Demand Ratio

https://www.comptia.org/newsroom/press-releases/2022/06/07/cybersecurity-hiring-momentum-ramps-up-new-data-from-cyberseek-reveals

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

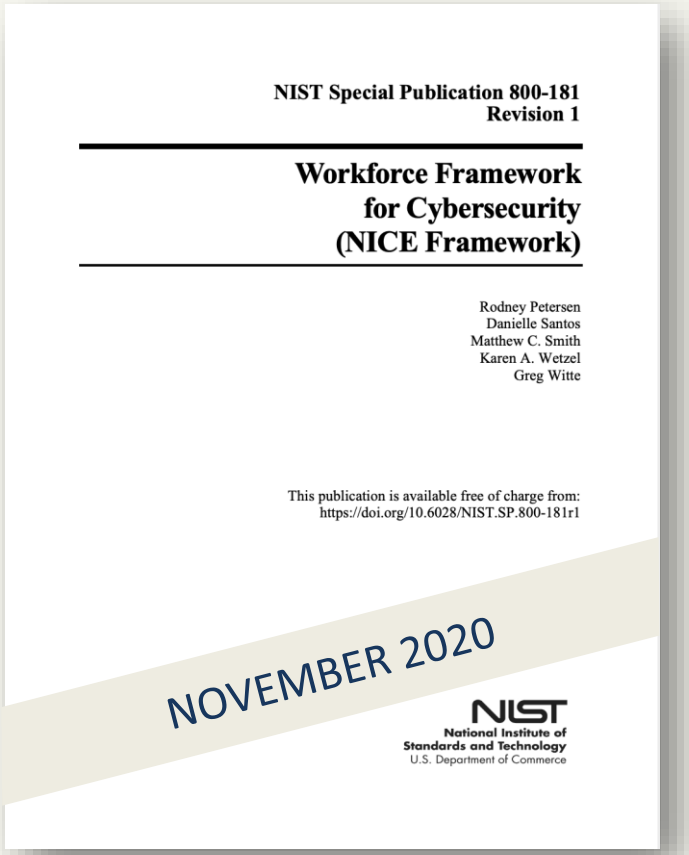
NICE Workforce Framework for Cybersecurity

- ✔ A common, consistent lexicon to **clearly share information** about cybersecurity work
- ✔ Direct information about **what a workforce needs to know**
- ✔ A **workforce skilled in cybersecurity**, not only a cybersecurity workforce
- ✔ Enables the establishment of **regular processes**
- ✔ For use in **career awareness**, **education and training**, **hiring and career development**, **workforce planning and assessment**

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

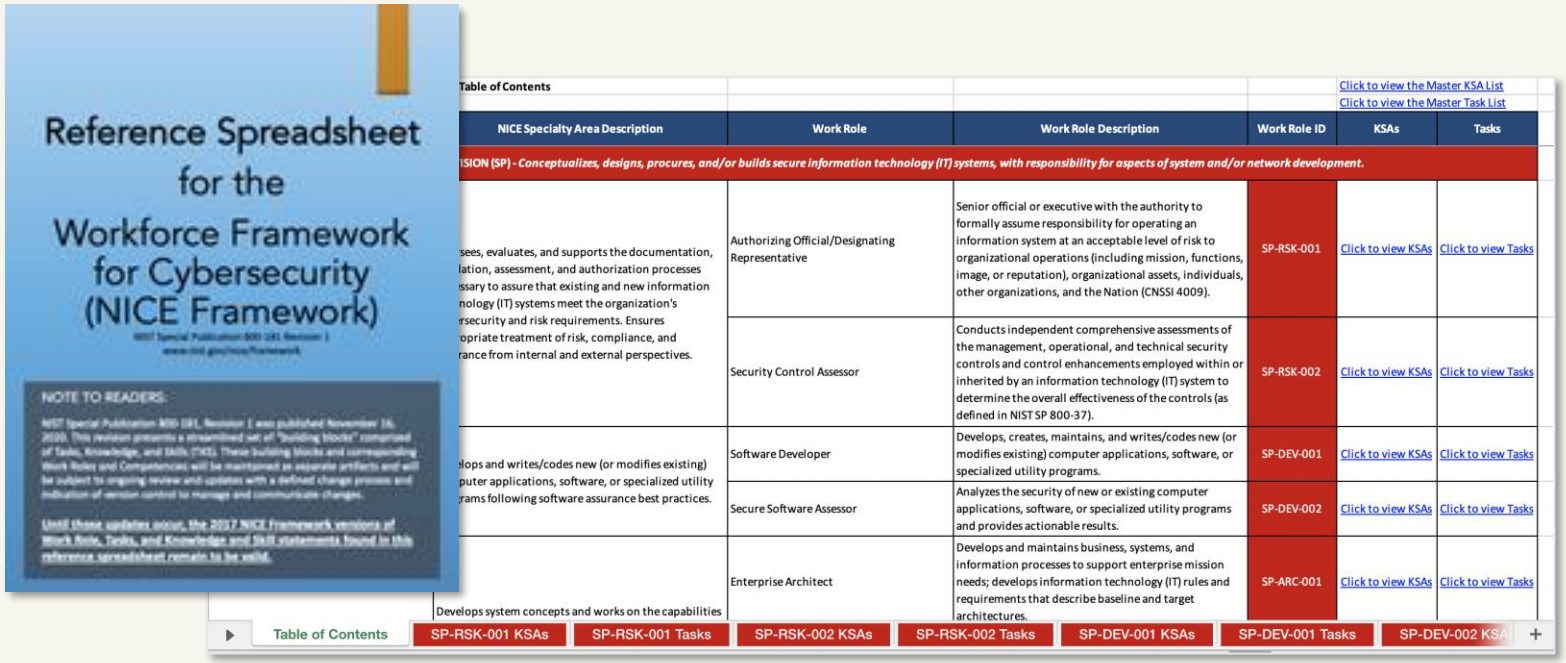
Workforce Framework for Cybersecurity (NICE Framework)

Framework Document



nist.gov/nice/framework

Reference Spreadsheet



www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-supplemental-material

Required Adoption in the Federal Workforce

- **Federal Cybersecurity Workforce Assessment Act (2015)**
  Requires agencies to:
  - Identify and code positions using the NICE Framework
  - Identify and annually report on cybersecurity work roles of critical need through 2022

- **Executive Order on America's Cybersecurity Workforce (May 2019)**
  Extends adoption to federal contractors:
  - Incorporate NICE Framework into workforce knowledge and skill requirements in contracts for IT and cybersecurity services
  - Use the NICE Framework in evaluating personnel
  - Incorporate the NICE Framework into existing education, training, and workforce development efforts

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Attributes

Agility

People, processes, and technology mature and must adapt to change. The NICE Framework enables organizations to keep pace with a constantly evolving ecosystem.

Flexibility

There is no one-size-fits-all solution to common challenges. The NICE 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. The NICE Framework enables organizations to exchange workforce information using a common language.

Modularity

In addition to cybersecurity, organizations manage other risks within the enterprise. The NICE Framework enables communication about these other workforces (e.g., privacy) within the enterprise and across sectors.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Who is the NICE Framework For?

- Public and Private Sectors
- Human Resources
- Hiring Managers
- Other SME's

EMPLOYERS

- Students
- Job-Seekers
- Employees

LEARNERS

- Learning Pathways
- Credentials

EDUCATION, TRAINING, AND CREDENTIAL PROVIDERS

Government • Industry • Academia

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

HOW CAN I USE THE NICE FRAMEWORK?

Employers

- Track workforce capabilities
- Create position descriptions
- Assess learner capabilities
- Develop teams

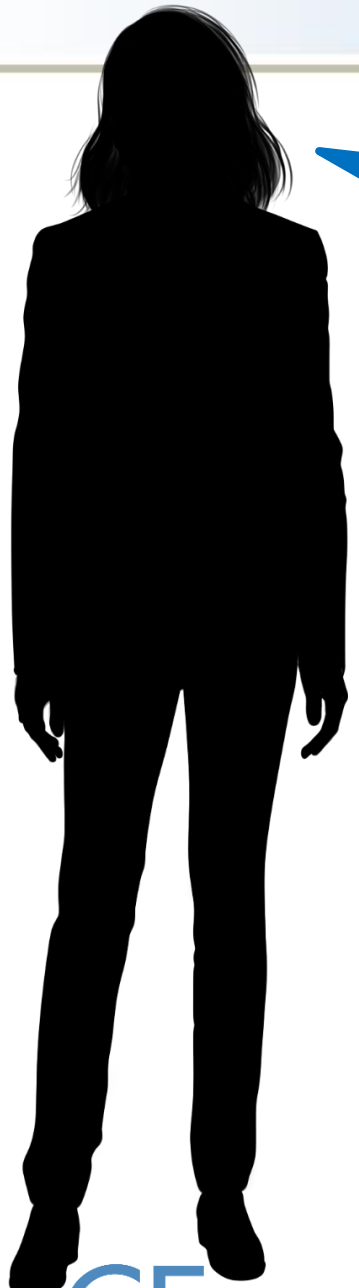
Education & Training Providers

- Develop a learning program
- Align teaching with NICE Framework
- Assess whether learners have achieved capabilities

Learners (students, job-seekers, & employees)

- Learn about a defined area of expertise
- Find out about what an organization needs
- Self-assessment

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION



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

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

How can we be sure to hire the right candidate?

Solution: Use the NICE Framework to…

- Identify Competency Areas & 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

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

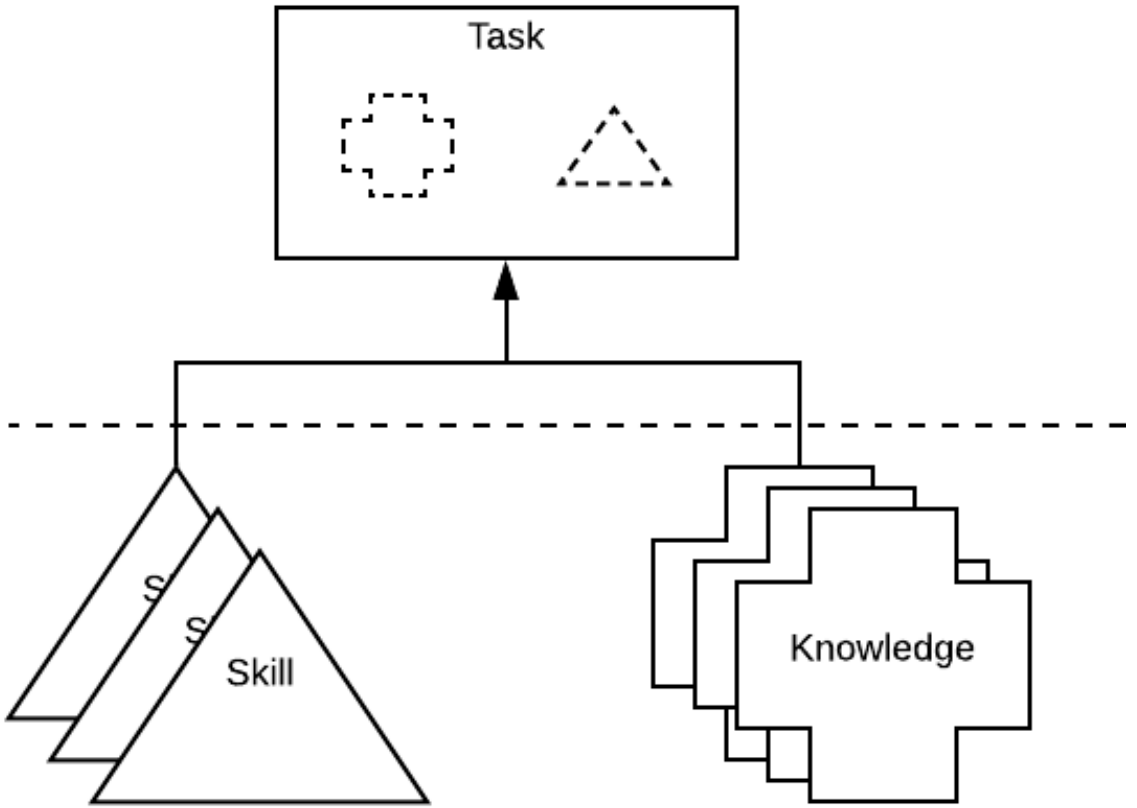
I'm looking to shift to a new cybersecurity role in my organization but want to make sure I'm prepared.

Solution: Upskill and reskill with the NICE Framework

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

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

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



Describes the Work

Describes the Learner

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Using the NICE Framework: Building Block Applications

TEAMS

- Defined by Competencies or Work Roles

COMPETENCY AREAS

- Groupings of TKS statements
- Means of assessing or demonstrating capability

WORK ROLES

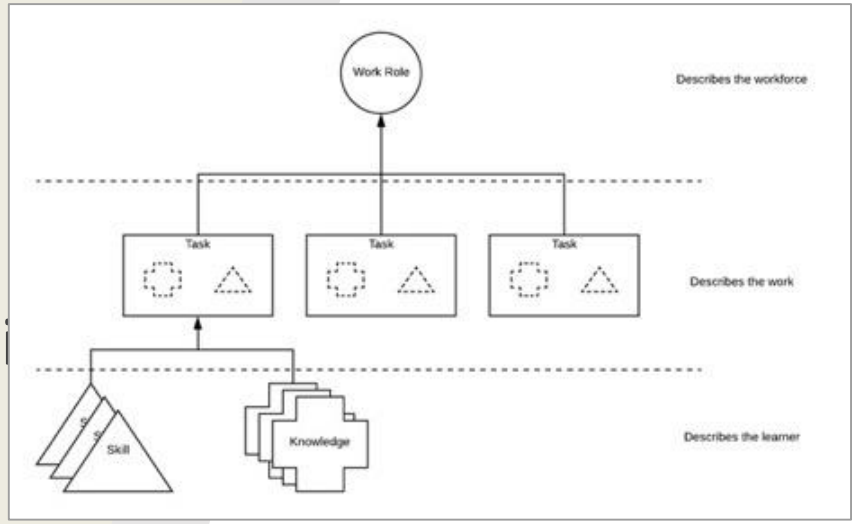
- Groupings of Task statements
- Work someone is responsible for

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Work Roles

Work Role:

A grouping of work for which someone is responsible or accountable



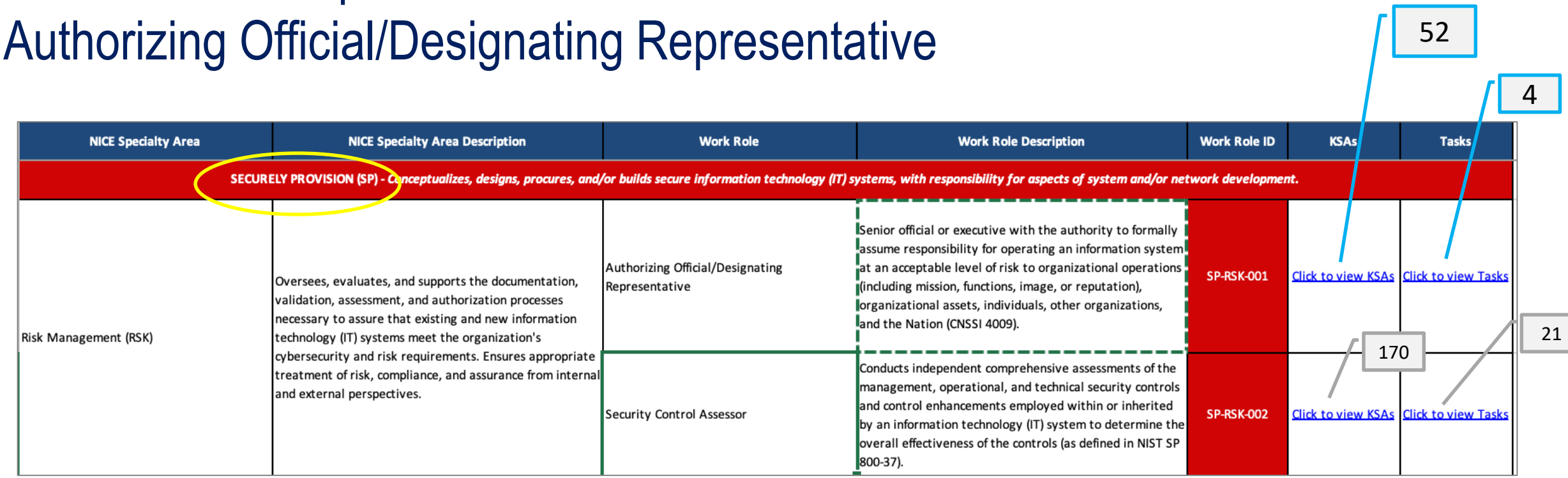
Work Roles:

- Are not synonymous with job titles or occupati
- 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

Work Role Example:
Authorizing Official/Designating Representative



NICE Specialty Area	NICE Specialty Area Description	Work Role	Work Role Description	Work Role ID	KSAs	Tasks
SECURELY PROVISION (SP) - Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.						
Risk Management (RSK)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new information technology (IT) systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.	Authorizing Official/Designating Representative	Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation (CNSSI 4009).	SP-RSK-001	Click to view KSAs	Click to view Tasks
		Security Control Assessor	Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).	SP-RSK-002	Click to view KSAs	Click to view Tasks

Task ID	Task
T0145	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
T0371	Establish acceptable limits for the software application, network, or system.
T0495	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Why Competency Areas?

- 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

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Framework Competency Areas

What are they?

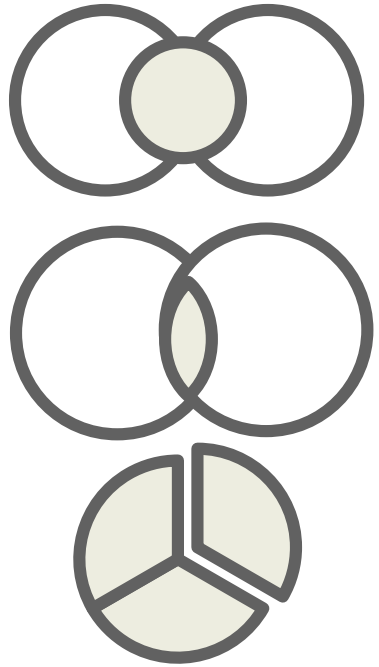
Measurable clusters of related Task, Knowledge, or Skill (TKS) statements in a particular domain that correlates with performance on the job and can be improved through education, training (including on-the-job and via apprenticeships), or other learning experiences.

Competency Areas are:

- Defined via an employer-driven approach
- Learner-focused
- Can apply to multiple Work Roles, although a Work Role can also stand independent of the Competency Area

Consist of:

Title • Description • TKS statements



2nd Draft NISTIR 8355
NICE Framework Competencies: Assessing Learners for Cybersecurity Work
https://doi.org/10.6028/NIST.IR.8355-draft2

How Do Competencies Differ from Work Roles?

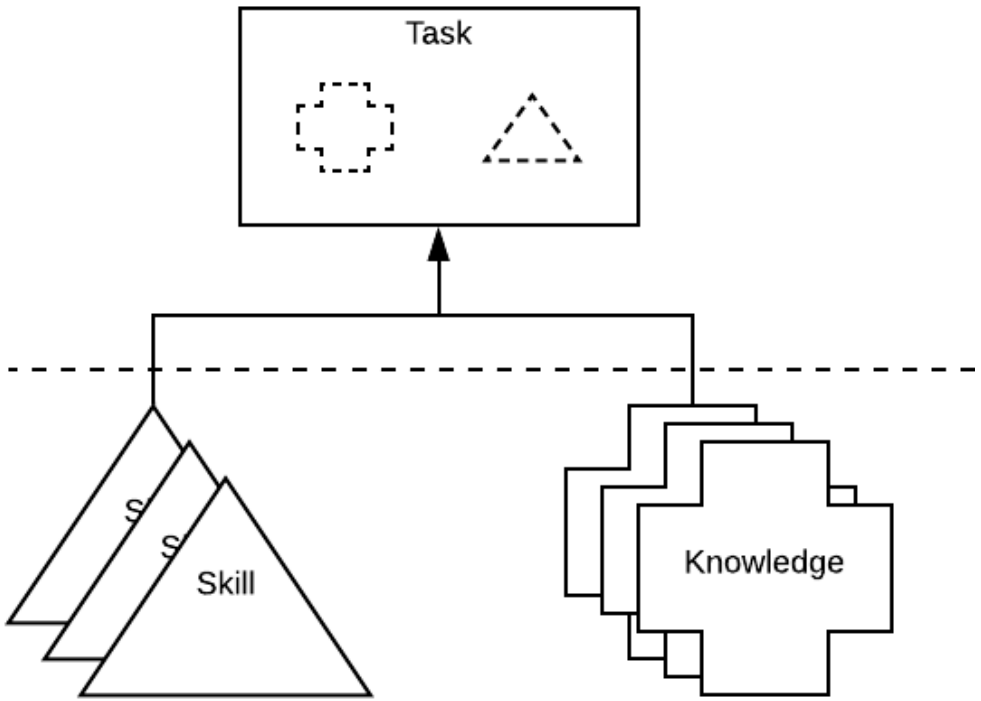
Competency Areas

- Learner focused
- Help address employer needs
- Assessment is typically based on the Competency Area as a whole

Work Roles

- Work focused
- Help define positions and responsibilities
- Assessment typically occurs at the task level

TKS Statements:
NICE Framework Building Blocks



Competency Areas: Measurable clusters of related TKS statements in a particular domain.

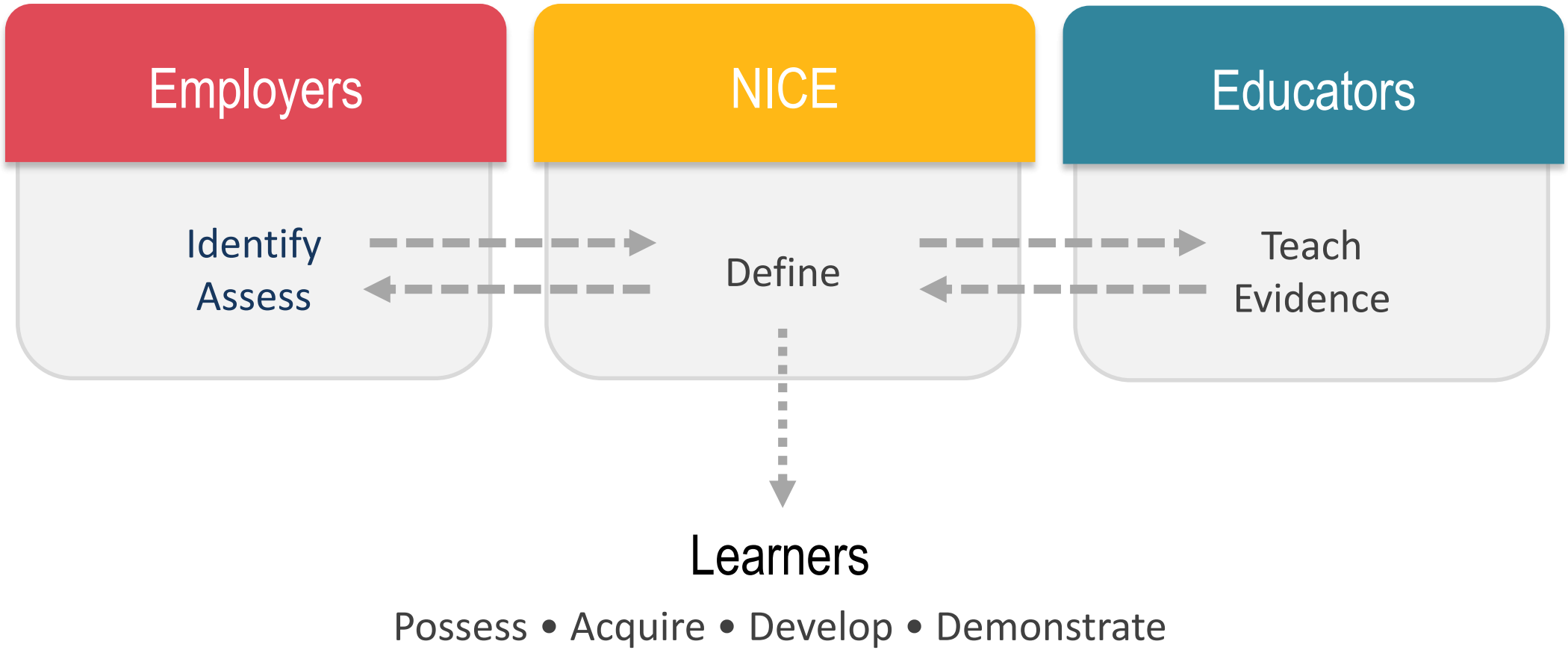
Work Roles: Groupings of tasks for which a person or team is responsible.

focus on **Work Roles**

focus on **Competency Areas**

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Competency Areas: Stakeholders

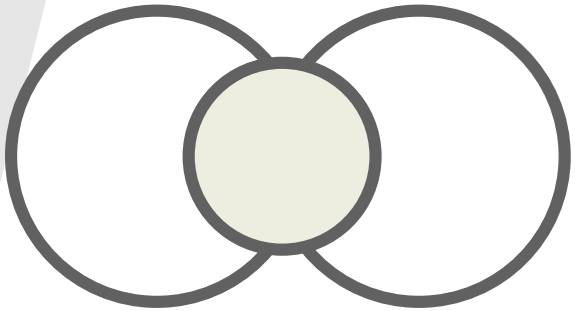


NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Applying Competency Areas

Overlaid on Work Role(s)

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



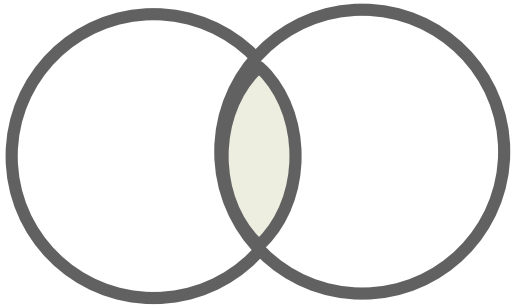
Example:

Cloud Security Competency Area + Security Architect Work Role

Applying Competency Areas

Common Ground for communication and coordination

- For effectiveness 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:

Operational Technology Security Competency Area *needed by:*

- Facilities Manager
- Information Systems Security Developer

Applying Competency Areas

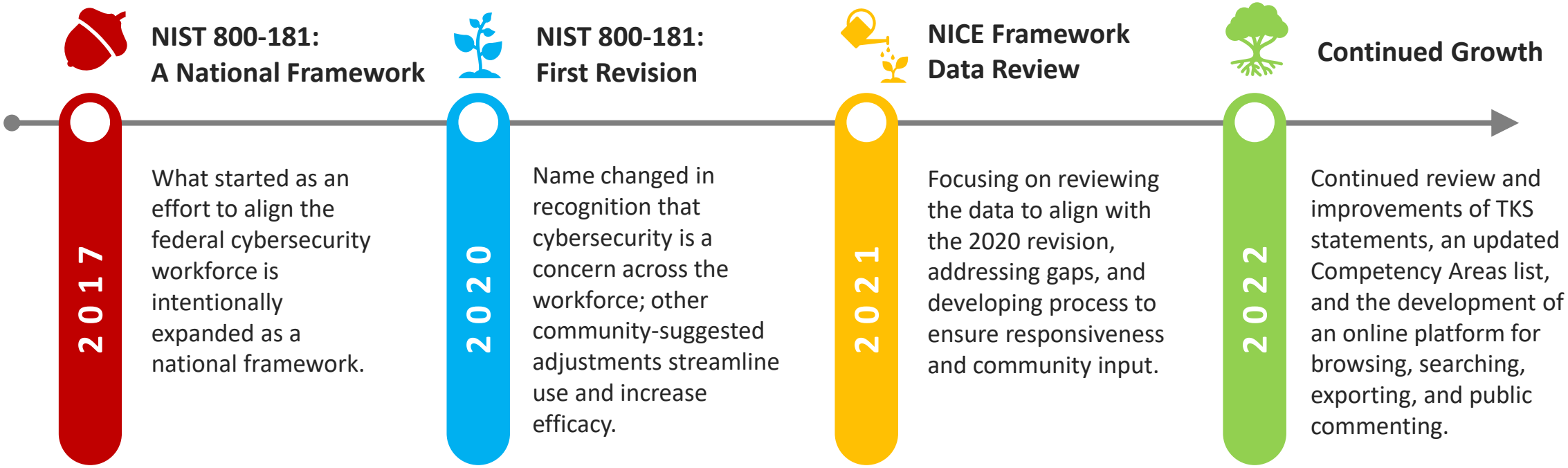
Learning for students, job-seekers, or employees

- 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

Example:

Digital Forensics Competency Area

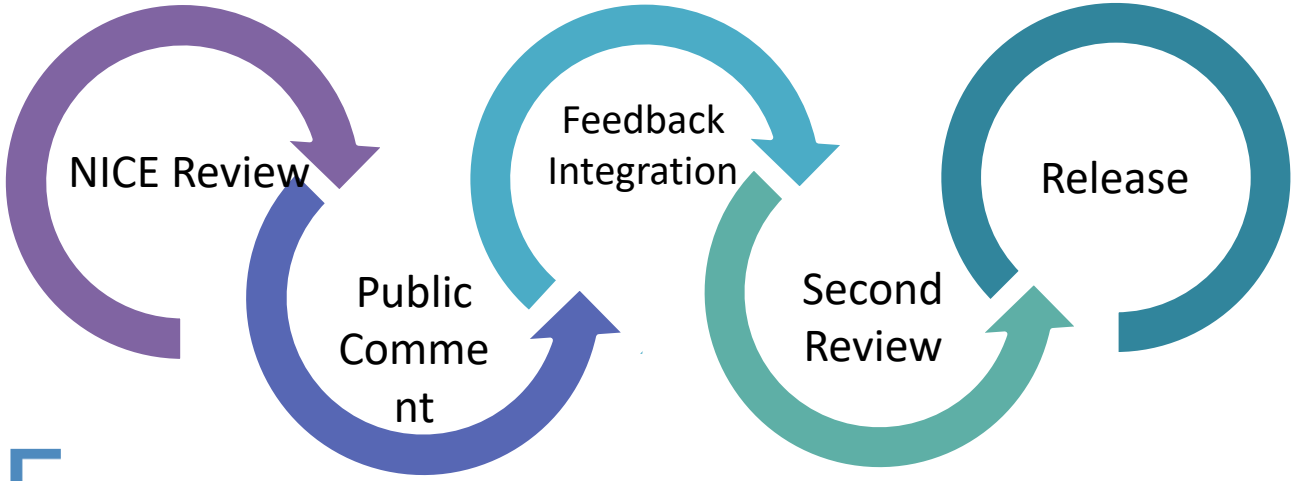
NICE Framework Evolution



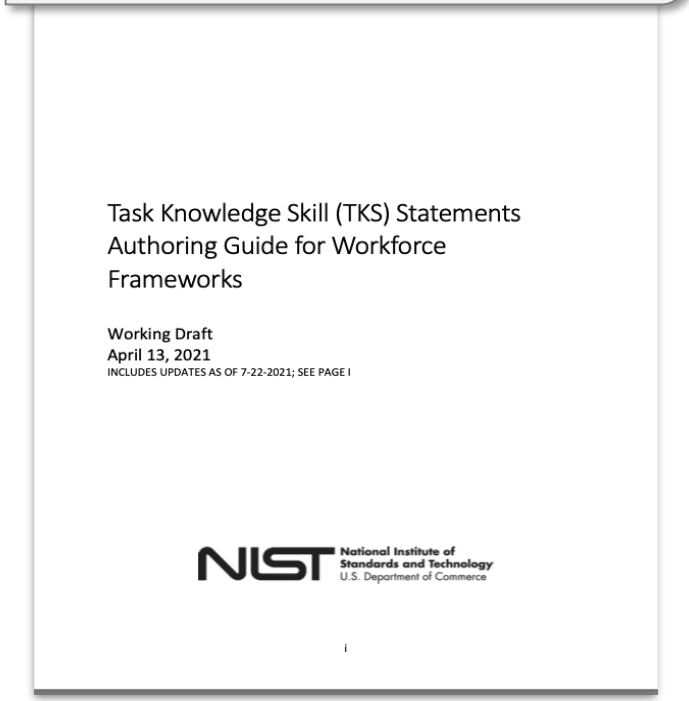
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICE Statement Updates

- **Ability Statements:** Refactored as Skill (primarily), Knowledge, or Task statements
- **Knowledge and Skill statements:** Updates to introduce consistency and clarity and to address redundancies
- **Task statements:** Consistency, clarity – *initial review has just begun*



TKS Authoring Guide for Workforce Frameworks


Task Knowledge Skill (TKS) Statements Authoring Guide for Workforce Frameworks

Working Draft
April 13, 2021
INCLUDES UPDATES AS OF 7-22-2021; SEE PAGE I

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

i

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Ongoing 2022 Priorities

- Updated NICE Framework Competency Areas
- Operational Technology (OT) content integration
- Cybersecurity Awareness Work Role
- Task Review and K&S Alignment
- NIST data platform
  - Online access to NICE Framework data (browse/search/download)
  - Public comment tool
  - Ongoing maintenance
- Alignment with related frameworks
- Work Roles and Categories review
- Supporting resources: Quickstart guide, etc.
- Workshops: NICE Framework tools, high-performing teams, other ideas?

Sample Tools & Applications

www.nist.gov/nice/framework

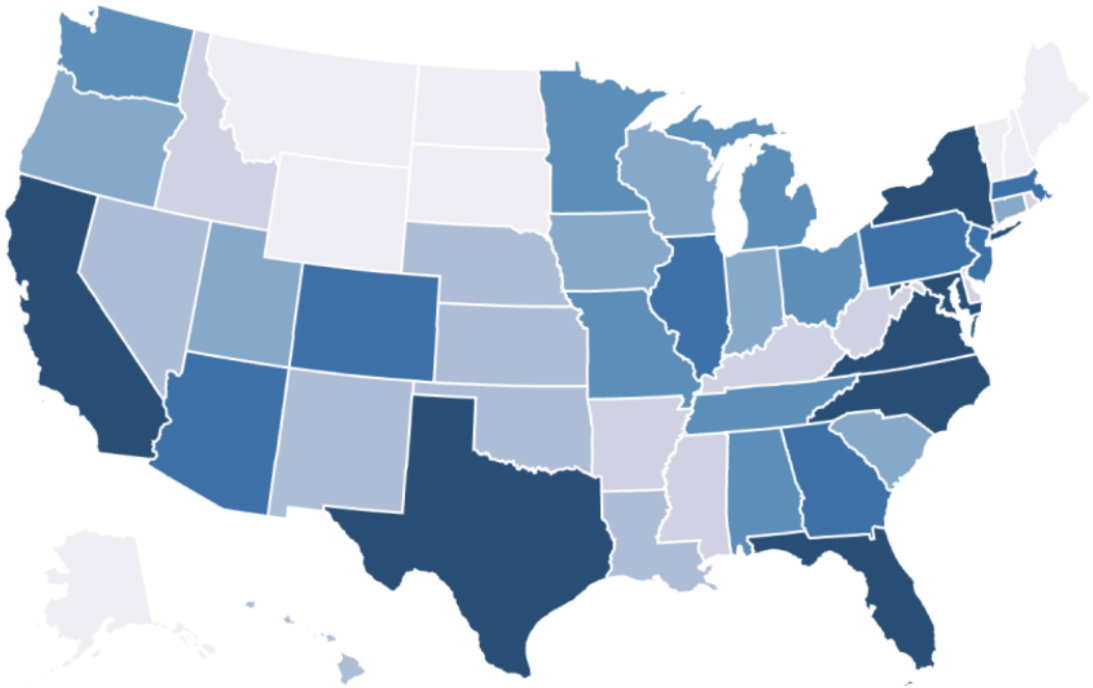
- **CyberSeek:** An interactive cybersecurity jobs heat map and career pathway tool. Jobs across the U.S. by state and metropolitan and how they align to the NICE Framework.
- **NICE Framework Keyword Search**
- **NICE Framework Mapping Tool**: Answer questions about your federal cybersecurity-related 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:** An interactive way to explore NICE Framework Work Roles. 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.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

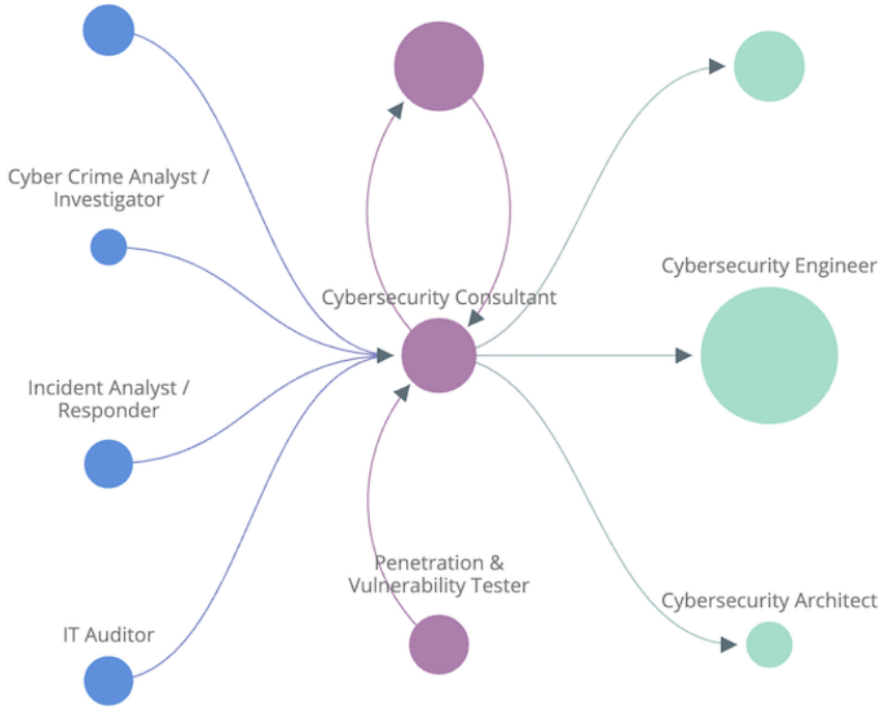
CyberSeek™

To help close the cybersecurity skills gap, CyberSeek provides detailed, actionable data about supply and demand in the cybersecurity job market.

Interactive Map



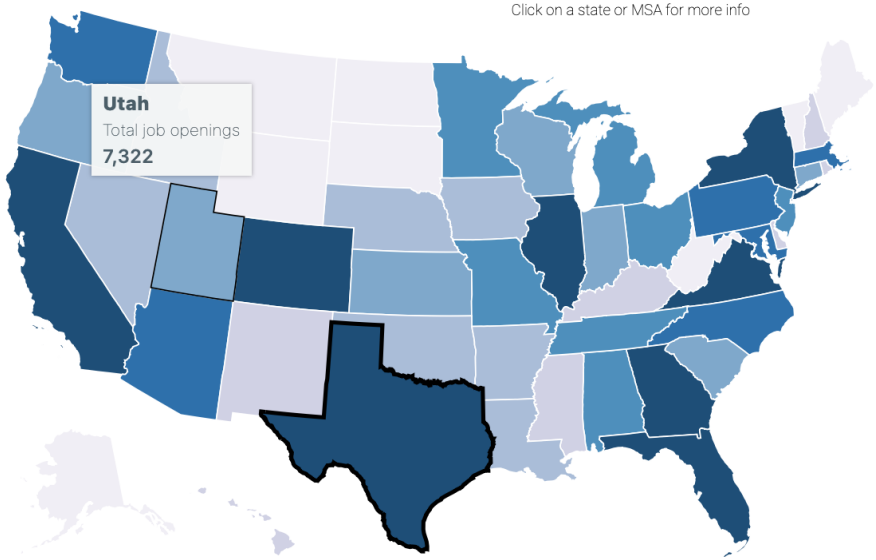
Career Pathway



Cyberseek.org - Interactive Heat Map and Career Pathway Tool

CyberSeek™

Click on a state or MSA for more info



TOTAL JOB OPENINGS

- 555 - 1,786
- 1,787 - 4,084
- 4,085 - 6,404
- 6,405 - 7,860
- 7,861 - 16,601
- 16,602 - 24,986
- 24,987 - 83,126

Texas

TOTAL CYBERSECURITY JOB OPENINGS

83,126

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

104,791

SUPPLY/DEMAND RATIO

High Supply

Low Supply

◀66% National average

GEOGRAPHIC CONCENTRATION

High

LOCATION QUOTIENT

TX 1.5

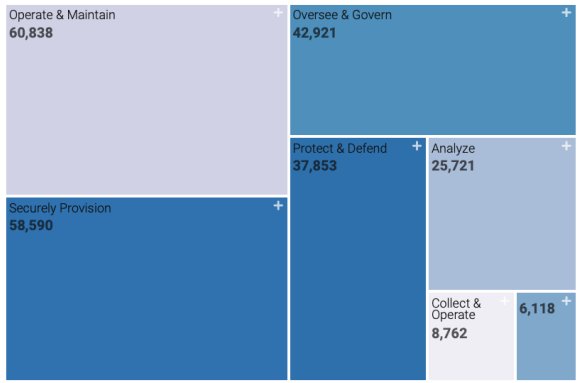
National average 1.0

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

NICE



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

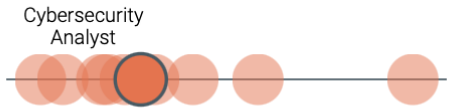
NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Cyber Seek Example: Cybersecurity Analyst Detail View

Cybersecurity Analyst

AVERAGE SALARY

$107,500



COMMON JOB TITLES

- Security Analyst
- Information Security Analyst
- Information Technology Security Analyst
- Security Operations Analyst
- Compliance Analyst

REQUESTED EDUCATION (%)

TOTAL JOB OPENINGS

36,732

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 (CISSP)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Information Security Manager (CISM)

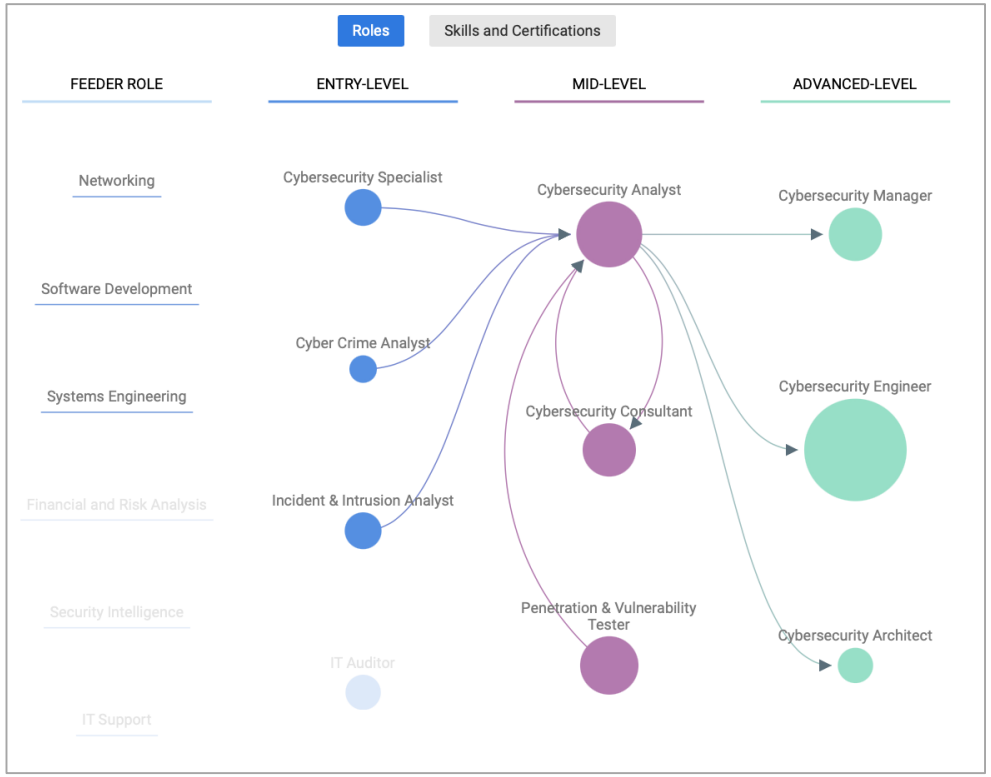
TOP SKILLS REQUESTED

1. Information Security
2. Information Systems
3. Linux
4. Network Security
5. Threat Analysis
6. Security Operations
7. Vulnerability assessment
8. Project Management
9. Intrusion detection

CyberSeek™

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

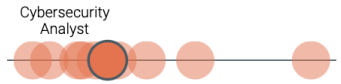
Cyber Seek Cybersecurity Career Pathway: Cybersecurity Analyst



Cybersecurity Analyst

AVERAGE SALARY

$107,500



COMMON JOB TITLES

- Security Analyst
- Information Security Analyst
- Information Technology Security Analyst
- Security Operations Analyst
- Compliance Analyst

REQUESTED EDUCATION (%)

TOTAL JOB OPENINGS

36,732

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 (CISSP)
- SANS/GIAC Certification (Various)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Information Security Manager (CISM)

TOP SKILLS REQUESTED

1. Information Security
2. Information Systems
3. Linux
4. Network Security
5. Threat Analysis
6. Security Operations
7. Vulnerability assessment
8. Project Management
9. Intrusion detection

CyberSeek™

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NICCS Cyber Career Pathways Tool: Vulnerability Assessment Analyst

NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

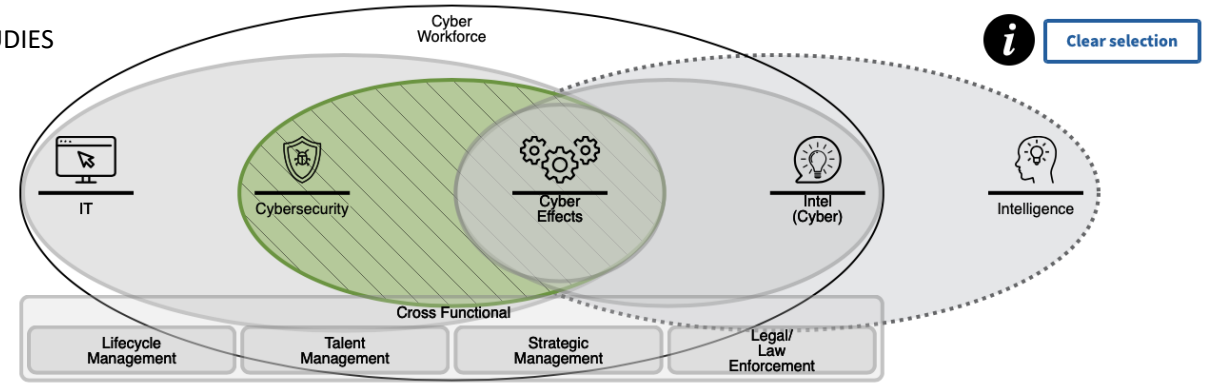
Cyber Career Pathways Tool

Welcome to the Cyber Career Pathways Tool!

This tool presents a new and interactive way to explore work roles within the Workforce Framework for Cybersecurity (NICE Framework). It depicts the Cyber Workforce according to five distinct, yet complementary, skill communities. It also highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and those considering a career in Cyber.

The Cyber Career Pathways Tool User Guide provides additional information on tool features and functionality.

To start, select a work role below, or enter keywords in the search bar.



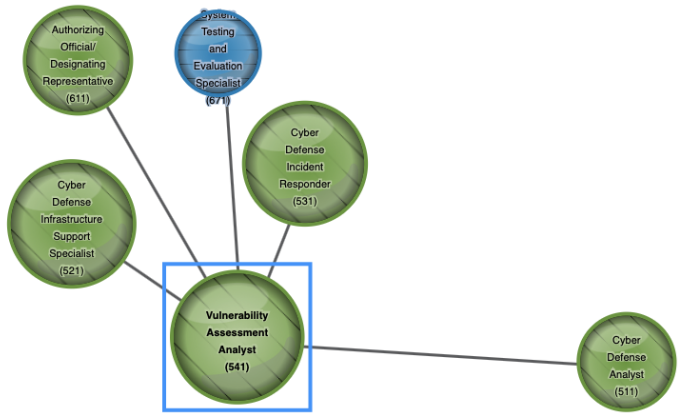
Clear selection

Vulnerability Assessment Analyst

Begin typing to search work role names. Or search job titles.

Compare against another Work Role

Search job titles.



Details

- Tasks
- KSAs
- Capability Indicators
- Common Relationships
- Federal Data

Vulnerability Assessment Analyst

Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Community: Cybersecurity
Category: Protect and Defend
Specialty Area: Vulnerability Assessment and Management
OPM ID: 541

See USAJOBS listings coded for Vulnerability Assessment 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.

- Blue Team Technician
- Computer Network Defense (CND) Auditor
- Ethical Hacker
- Information Security Engineer
- Network Security Engineer

NICCS Cyber Career Pathways Tool: Vulnerability Assessment Analyst

NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

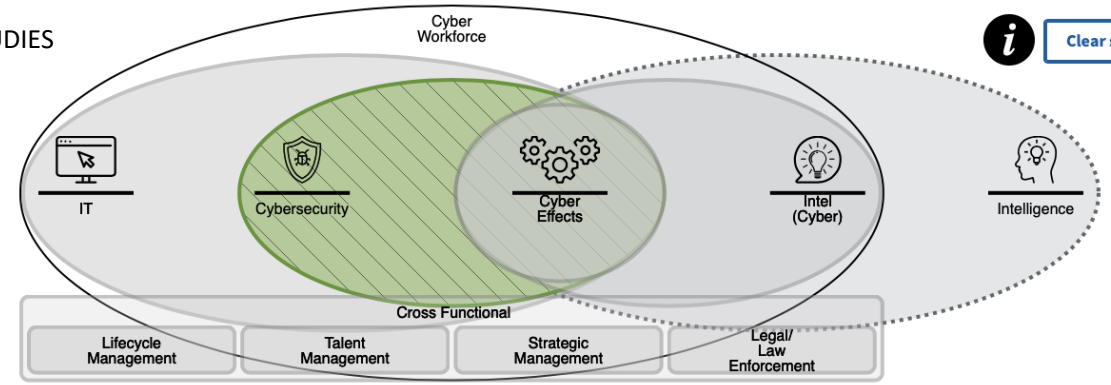
Cyber Career Pathways Tool

Welcome to the Cyber Career Pathways Tool!

This tool presents a new and interactive way to explore work roles within the Workforce Framework for Cybersecurity (NICE Framework). It depicts the Cyber Workforce according to five distinct, yet complementary, skill communities. It also highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and those considering a career in Cyber.

The Cyber Career Pathways Tool User Guide provides additional information on tool features and functionality.

To start, select a work role below, or enter keywords in the search bar.



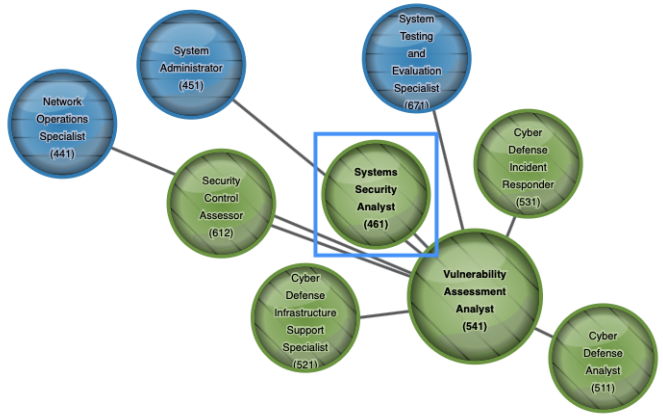
Clear selection

Vulnerability Assessment Analyst

Begin typing to search work role names. Or search job titles.

Compare against another Work Role

Search job titles.



Details
Tasks
KSAs
Capability Indicators
Common Relationships
Federal Data

Related Roles by KSAT | **On Ramps** | Off Ramps

The following work roles serve as common stepping stones to the selected work role as identified by subject matter experts for developing both linear and latticed career paths.

- Cyber Defense Analyst
- Cyber Defense Incident Responder
- Cyber Defense Infrastructure Support Specialist
- Network Operations Specialist
- Security Control Assessor
- System Administrator
- System Testing and Evaluation Specialist
- Systems Security Analyst

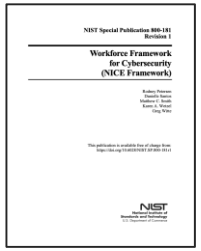
NICE Framework Resource Center

www.NIST.gov/NICE/Framework

1

NF Content & Tools

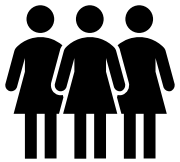
Framework Document
-
Supplemental Material
-
Updates
-
Tools



2

Resources by Stakeholder

Employers
-
Education & Training Providers
-
Learners



3

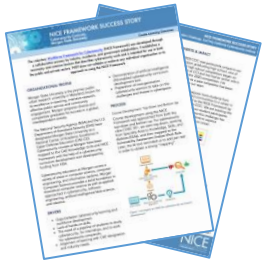
Users Group

Learn
-
Share
-
Discuss
-
Influence

4

Success Stories

Profile
-
Drivers
-
Process
-
Benefits & Impact



5

Framework in Focus

Practitioner Profile
-
Career Path
-
Advice

6

About

FAQs
-
History
-
Audience
-
Revision Process

THANK YOU

Karen Wetzel, Manager, NICE Framework
karen.wetzel@nist.gov

NICE Program: www.nist.gov/nice

NICE Framework Resource Center:
www.nist.gov/nice/framework

NICE Community:
https://www.nist.gov/itl/applied-cybersecurity/nice/community

Upcoming Events

www.nist.gov/itl/applied-cybersecurity/nice/events

July 26: Federal Cybersecurity Workforce Summit Webinar
Employee Development Through Rotational and Exchange Programs
Register Now

October 17-22: Cybersecurity Career Awareness Week
Website

November 15: FISSEA Fall Forum
Federal Information Security Educators (FISSEA) community
Register Now

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

SLIDESMANIA.CO