Image source: https://pixabay.com/photos/blockchain-globe-network-3537389/

Developing the Cybersecurity Workforce:

An Introduction to the NICE Framework

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

NICE Mission

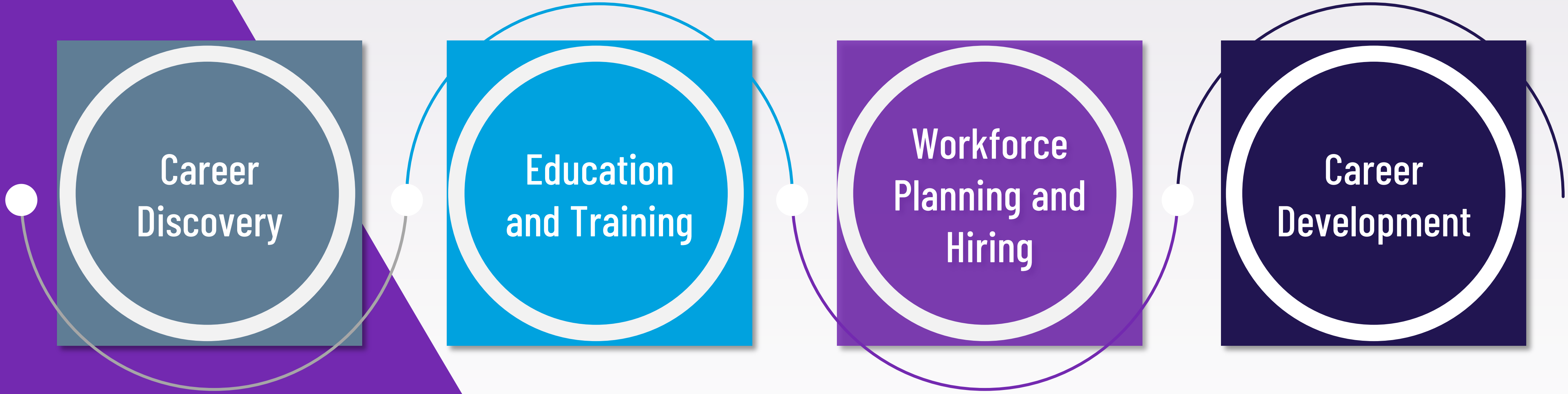
To energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

NIST NICE

About NICE

- 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
- Established by the Cybersecurity Enhancement Act of 2014, Title IV

NICE Focus Areas



Career Discovery

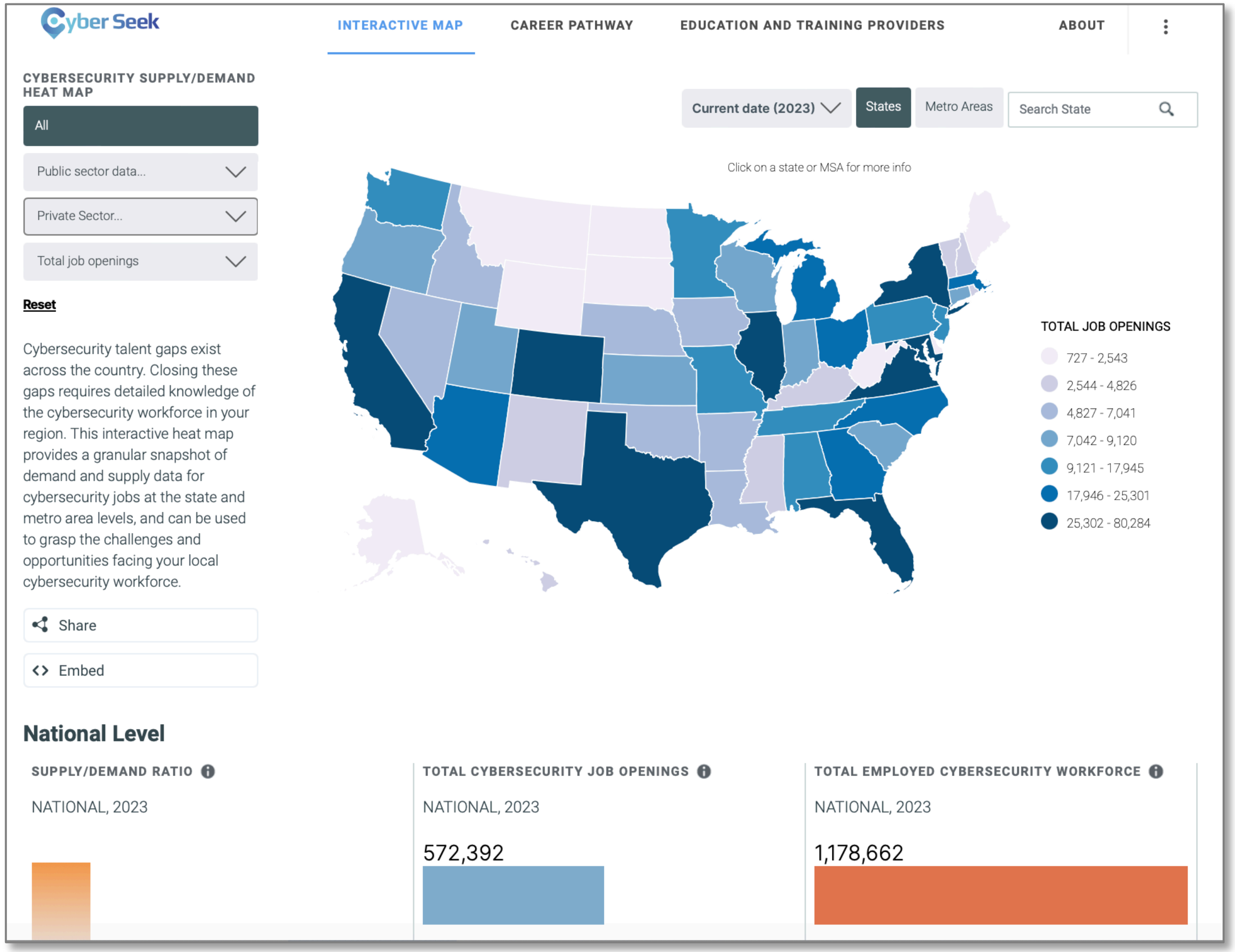
Education and Training

Workforce Planning and Hiring

Career Development

Cyberseek Cybersecurity Workforce Data

- **572,392** job openings
- **45,000** new postings each month
- **1,178,662** workers employed in cybersecurity-related jobs
- **315,000** more workers needed to close current supply gaps
- **72%** supply/demand ratio



CYBERSECURITY SUPPLY/DEMAND HEAT MAP

All

Public sector data...

Private Sector...

Total job openings

Reset

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

Embed

TOTAL JOB OPENINGS

- 727 - 2,543
- 2,544 - 4,826
- 4,827 - 7,041
- 7,042 - 9,120
- 9,121 - 17,945
- 17,946 - 25,301
- 25,302 - 80,284

National Level

SUPPLY/DEMAND RATIO

NATIONAL, 2023

TOTAL CYBERSECURITY JOB OPENINGS

NATIONAL, 2023

572,392

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

NATIONAL, 2023

1,178,662

Resource: www.CyberSeek.org

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

Image source: shutterstock.com

Image Source: https://pxhere.com/en/photo/1562171

Cybersecurity Workforce Opportunities

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

Good Jobs Principles

- Recruitment and Hiring
- Benefits
- Diversity, Equity, Inclusion, and Accessibility (DEIA)
- Worker Empowerment and Representation
- Job Security and Working Conditions
- Organizational Culture
- Living Wage
- Skills and Career Advancement

Department of Commerce and Department of Labor Good Jobs Principles
https://www.dol.gov/general/good-jobs/principles

Image source: shutterstock.com

Workforce Framework for Cybersecurity (NICE Framework)

NIST SP 800-181r1 (2020)

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.

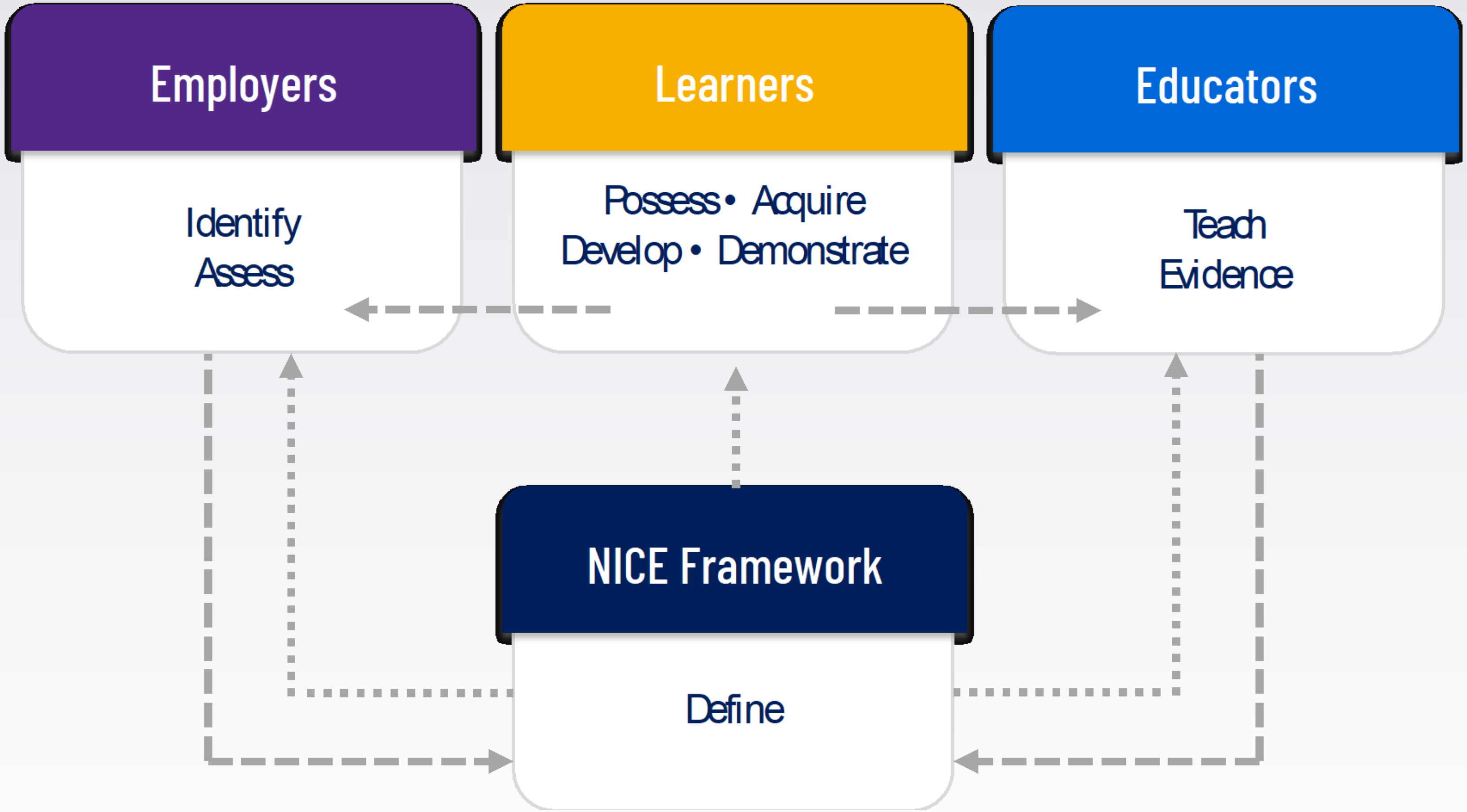
Interoperability

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.

NICE Framework:
Stakeholder Engagement



Employers

Identify
Assess

Learners

Possess • Acquire
Develop • Demonstrate

Educators

Teach
Evidence

NICE Framework

Define

NIST | NICE

https://freerangestock.com/photos/120801/handshake-between-two-people.html

Value for…

EMPLOYERS

- Broaden pipeline and increase diversity
- Create job descriptions and assess candidates
- Track and plan workforce capabilities
- Develop employees (WBL, training)

LEARNERS

- Discover and plan for cybersecurity careers
- Knowledge and skills development
- Demonstrate capability and evidence competency

EDUCATORS

- Develop learning courses and programs that address employer needs
- Align instruction with the NICE Framework
- Conduct performance-based assessments

GOVERNMENT • INDUSTRY • ACADEMIA

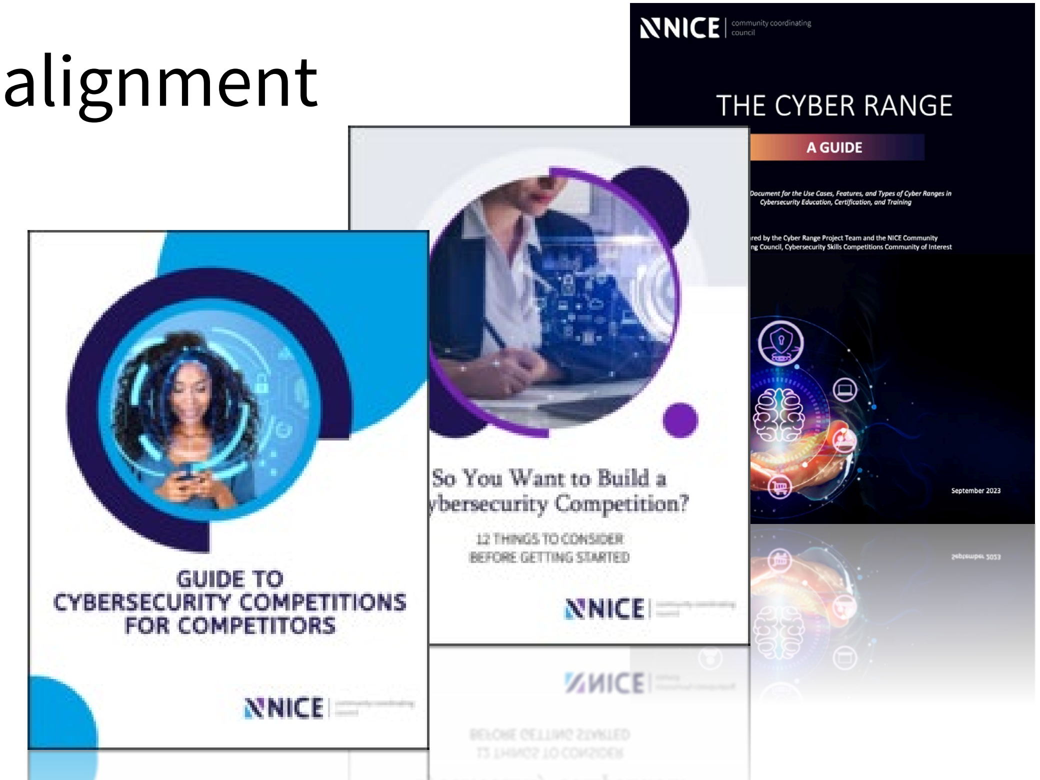
NICE Framework Relationships

- **National Frameworks, e.g.,**
  - NSF Workforce Framework for AI (in dev)
  - DCWF
  - CAE KUs
- **NIST Frameworks & Publications, e.g.,**
  - NIST Cybersecurity Framework
  - Privacy Framework & Workforce Framework for Privacy
  - Risk Management Framework
  - AI Risk Management Framework
  - Secure Software Development Framework
- **International Frameworks, e.g.,**
  - European Cyber Skills Framework (ECSF)
  - UK Cyber Career Framework
  - ASD Cyber Skills Framework
  - SFIA
  - Canadian Cybersecurity Skills Framework
- **Alignments & Mappings, e.g.,**
  - Certifications
  - Curriculum
  - Competitions (US Cyber Games, etc.)
  - Tools (Cyberseek, etc.)

Resource: Playbook for Workforce Frameworks

Cybersecurity Credentials & NICE Framework

- Cybersecurity Credentials Collaborative (C3) Certifications Mapping
- National Centers of Academic Excellence in Cybersecurity (NCAE-C) Program Mapping to the NICE Framework
- Cybersecurity Competitions, Cyber-Range alignment
- Curriculum development, pathway services, and more



NICE community coordinating council

THE CYBER RANGE

A GUIDE

Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification, and Training

red by the Cyber Range Project Team and the NICE Community ng Council, Cybersecurity Skills Competitions Community of Interest

September 2023

So You Want to Build a ybersecurity Competition?

12 THINGS TO CONSIDER BEFORE GETTING STARTED

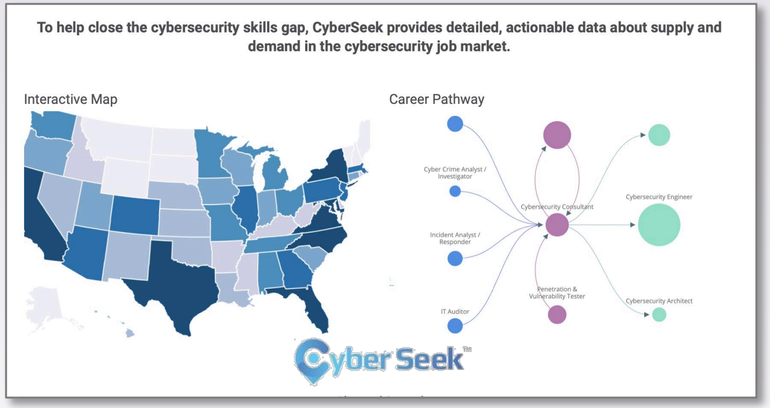
NICE

GUIDE TO CYBERSECURITY COMPETITIONS FOR COMPETITORS

NICE

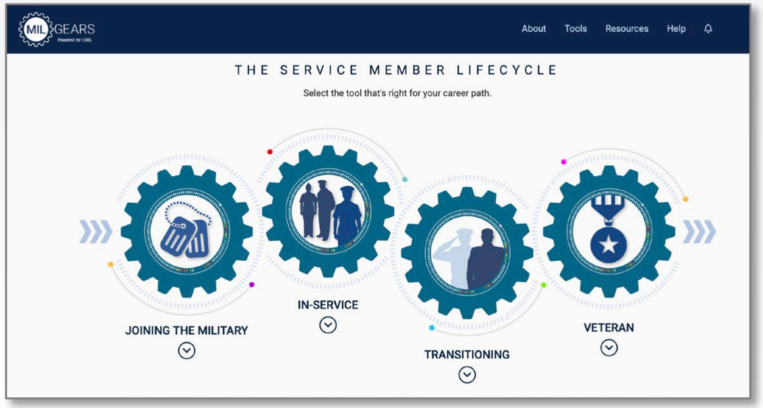
NIST NICE

Example NICE Framework Tools & Implementations



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

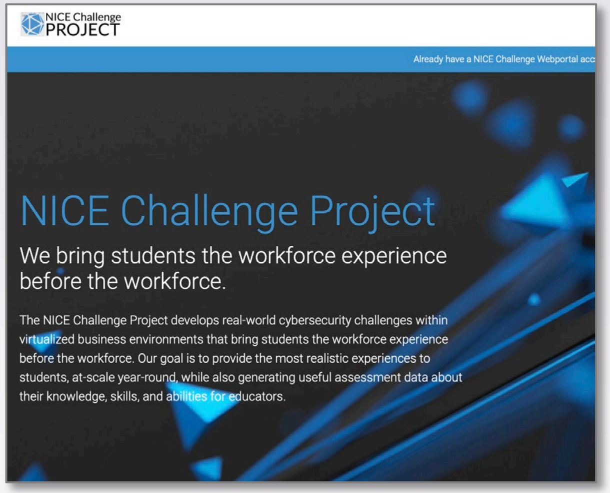
CyberSeek Jobs Map & Pathways



THE SERVICE MEMBER LIFECYCLE

Select the tool that's right for your career path.

MilGears

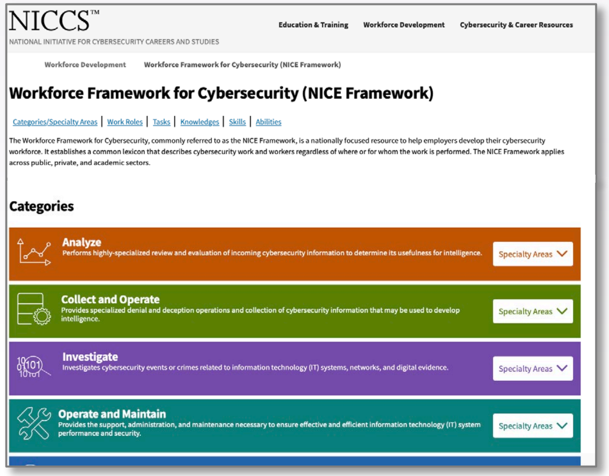


NICE Challenge Project

We bring students the workforce experience before the workforce.

The NICE Challenge Project develops real-world cybersecurity challenges within virtualized business environments that bring students the workforce experience before the workforce. Our goal is to provide the most realistic experiences to students, at-scale year-round, while also generating useful assessment data about their knowledge, skills, and abilities for educators.

NICE Challenge



NICCS™
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES
Education & Training
Workforce Development
Cybersecurity & Career Resources
Workforce Development
Workforce Framework for Cybersecurity (NICE Framework)

Workforce Framework for Cybersecurity (NICE Framework)

Categories/Specialty Areas | Work Roles | Tasks | Knowledges | Skills | Abilities

The Workforce Framework for Cybersecurity, commonly referred to as the NICE Framework, is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors.

Categories

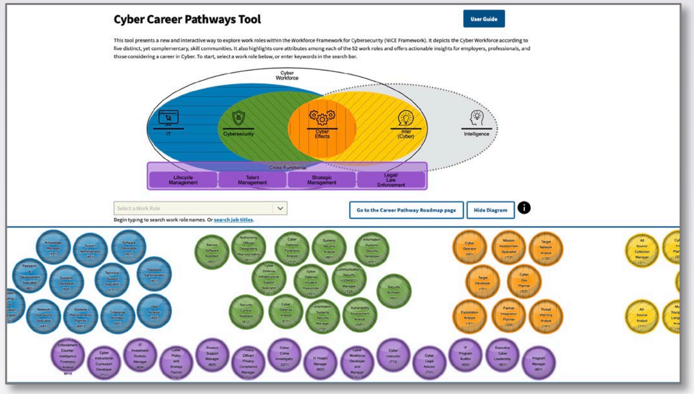
Analyze
Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Specialty Areas

Collect and Operate
Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Specialty Areas

Investigate
Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.
Specialty Areas

Operate and Maintain
Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Specialty Areas

NICE Framework Search

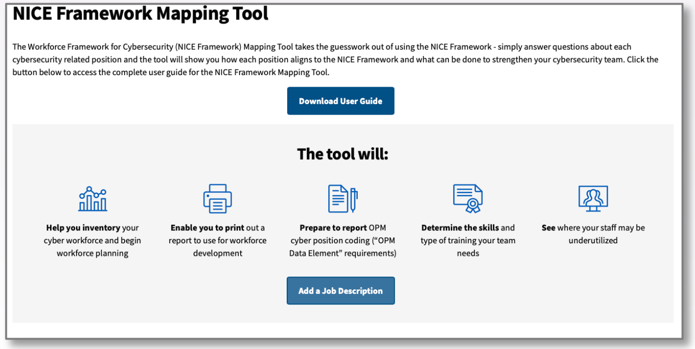


Cyber Career Pathways Tool

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

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

NICCS Career Pathways



NICE Framework Mapping Tool

The Workforce Framework for Cybersecurity (NICE Framework) Mapping Tool takes the guesswork out of using the NICE Framework - simply answer questions about each cybersecurity related position and the tool will show you how each position aligns to the NICE Framework and what can be done to strengthen your cybersecurity team. Click the button below to access the complete user guide for the NICE Framework Mapping Tool.

The tool will:

- **Help you inventory** your cyber workforce and begin workforce planning
- **Enable you to print** out a report to use for workforce development
- **Prepare to report** OPM cyber position coding ("OPM Data Element" requirements)
- **Determine the skills** and type of training your team needs
- **See** where your staff may be underutilized

Job Mapping

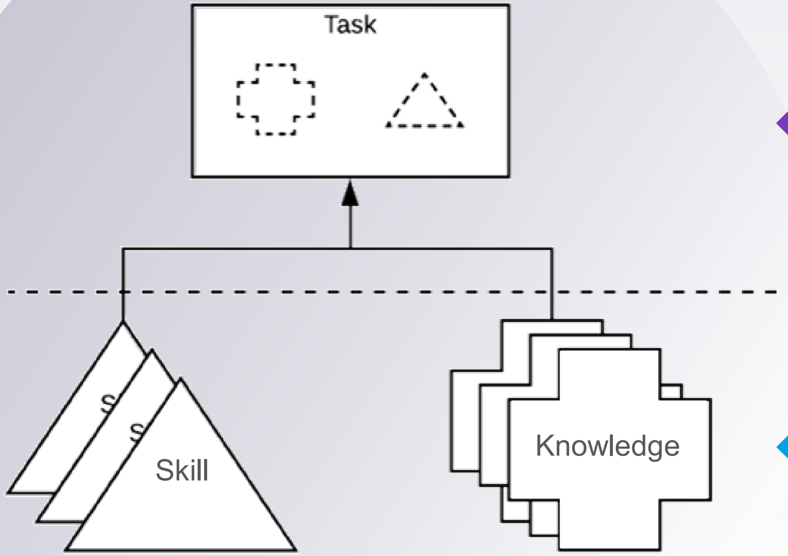
Resource: NICE Framework Resource Center

Image source: shutterstock.com

NICE Framework Components

TKS Statements,
Work Roles, and Competency Areas

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



Describes the Work

Describes the Learner

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.

Resource: NICE Framework Current Version

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

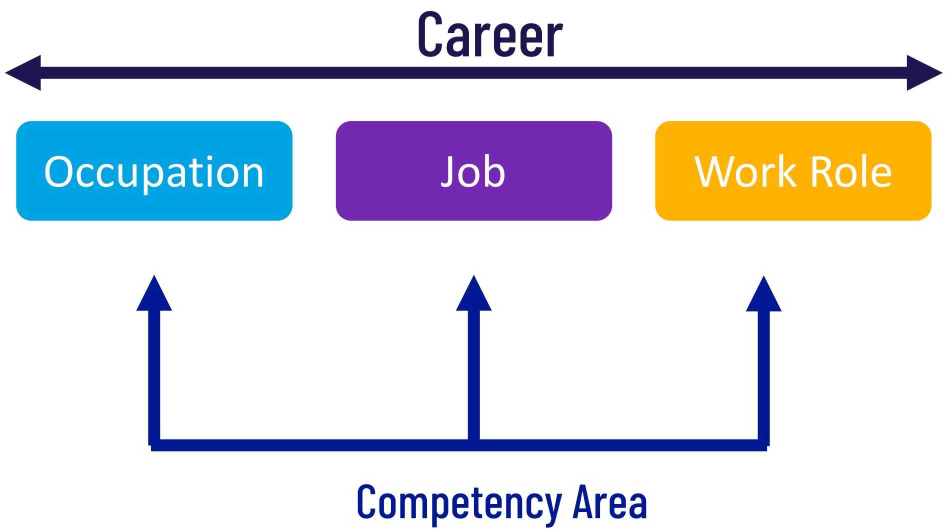
Images Sources:
https://creativecommons.org/licenses/by-sa/2.0
https://pixabay.com/photos/person-mountain-top-achieve-1245959/
https://pxhere.com/en/photo/1433389

NICE Framework Work Roles

What is a Work Role?

A grouping of work for which someone is responsible or accountable

- Are not synonymous with job titles or occupations
- A single job may comprise multiple roles (or partial)



Work Roles Consist of:

- Tasks that constitute the work to be done

They are used in:

- ➢ Career discovery & education
- ➢ Job descriptions & announcements
- ➢ Workforce planning & assessment
- ➢ Career pathways & development

NICE Framework Work Role Categories

and example roles*

NICE Framework
Work Role Categories
52 Work Roles
selected examples shown here

OVERSIGHT & GOVERNANCE	Policy and Planning, Security Control Assessment
DESIGN & DEVELOPMENT	Security Architect, Systems Development
IMPLEMENTATION & OPERATION	Database Administration, Network Management
PROTECTION & DEFENSE	Defensive Cybersecurity, Incident Response
INVESTIGATION	Cybercrime Investigation, Digital Evidence Forensics
INTELLIGENCE	All-Source Analysis, Intelligence Planning
CYBER EFFECTS	Cyber Operations, Target Development

Image source: shutterstock.com

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

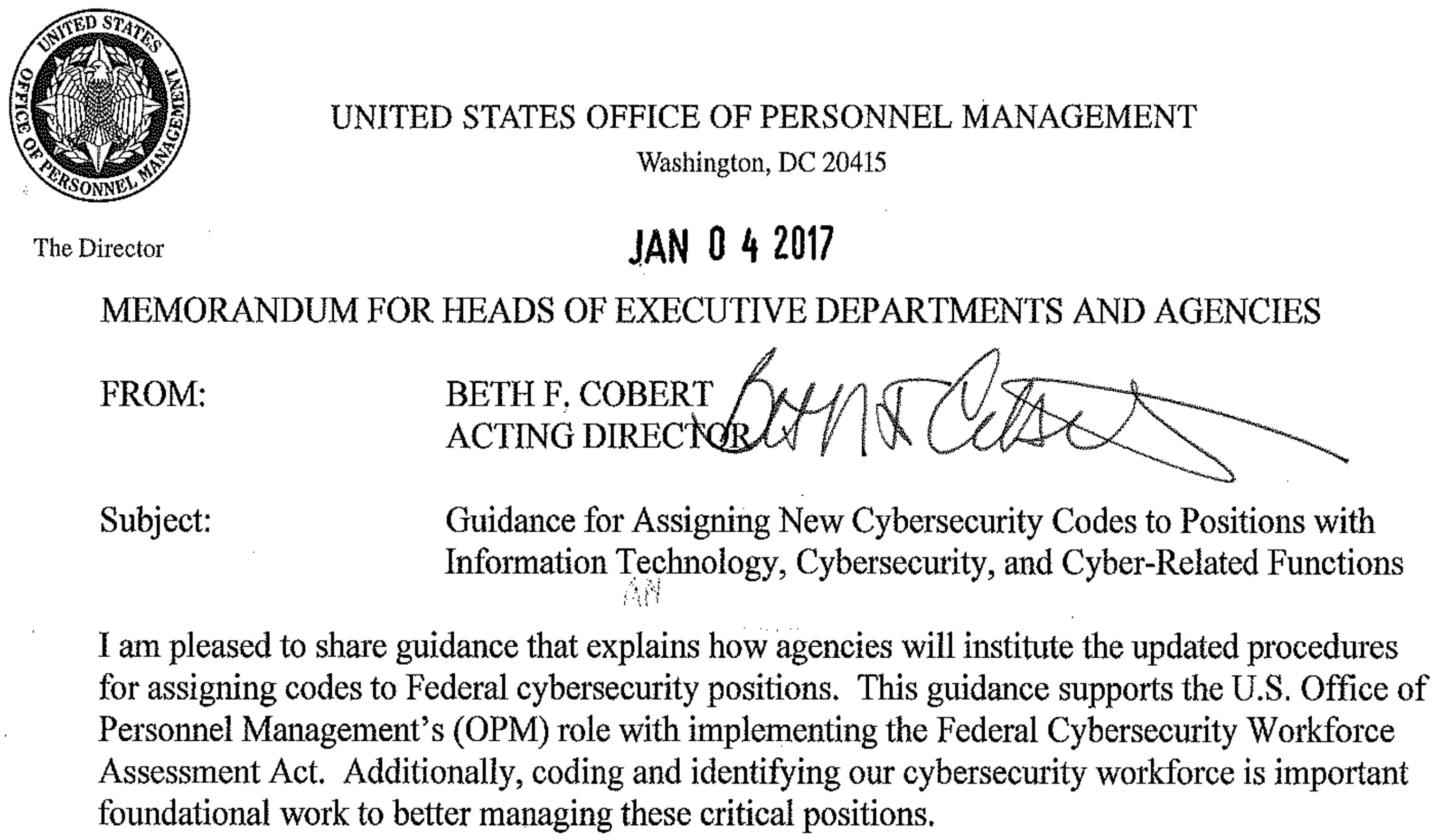
NICE Framework
Work Role Examples

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.
• 17 Tasks • 40 Knowledge/Skill/Ability	• 53 Tasks • 59 Knowledge/Skill/Ability	• 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.

Guidance for Assigning Cybersecurity Work Role Codes



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

JAN 0 4 2017

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: BETH F. COBERT
ACTING DIRECTOR

Subject: Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions

I am pleased to share guidance that explains how agencies will institute the updated procedures for assigning codes to Federal cybersecurity positions. This guidance supports the U.S. Office of Personnel Management's (OPM) role with implementing the Federal Cybersecurity Workforce Assessment Act. Additionally, coding and identifying our cybersecurity workforce is important foundational work to better managing these critical positions.

Cybersecurity Position Coding: Benefits

- Identifying critical needs
- Enhancing recruitment and hiring
- Justifying action to retain or gain critical skills
- Supporting training and development

Image source: shutterstock.com

Example Use: Hiring

Common Challenges

Unclear workforce needs

Working without a detailed position description

Conducting a candidate search with unrealistic goals

Employer’s Guide (2023)

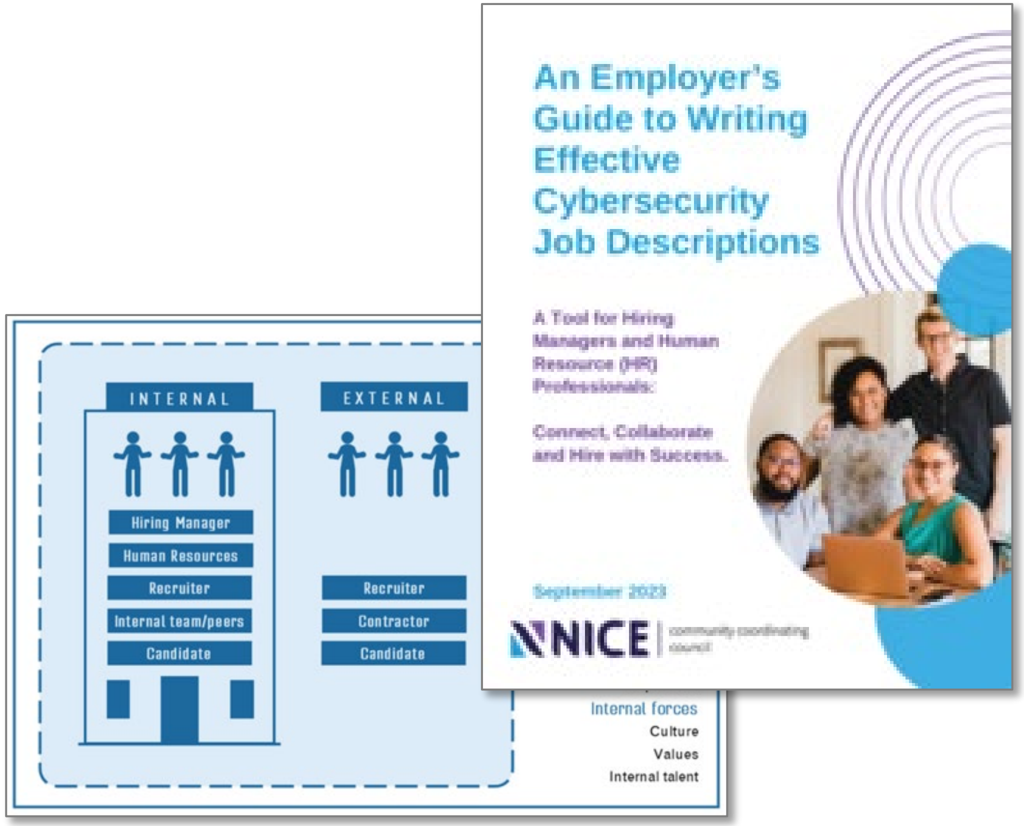
Three-step Approach:

1. Define Hiring Criteria
2. Define the Job
3. Candidate Assessment

Hiring Ecosystem

Community, environment, and the resulting interconnections needed to recruit employees into an organization. Includes:

- Human components
- Institutional processes
- Different technologies



An Employer’s Guide to Writing Effective Cybersecurity Job Descriptions

A Tool for Hiring Managers and Human Resource (HR) Professionals:

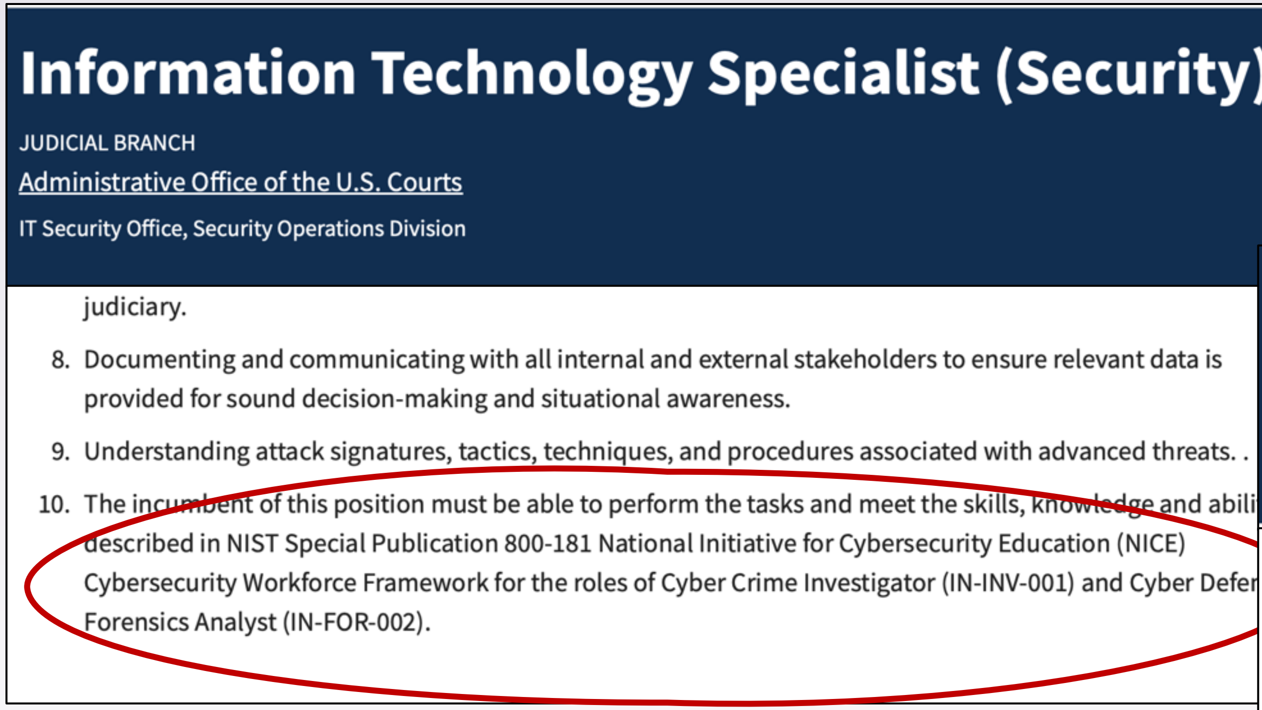
Connect, Collaborate and Hire with Success.

September 2023

NICE | community coordinating council

Resource: NICE Modernize Talent Management Working Group

USAJobs Examples



Information Technology Specialist (Security)

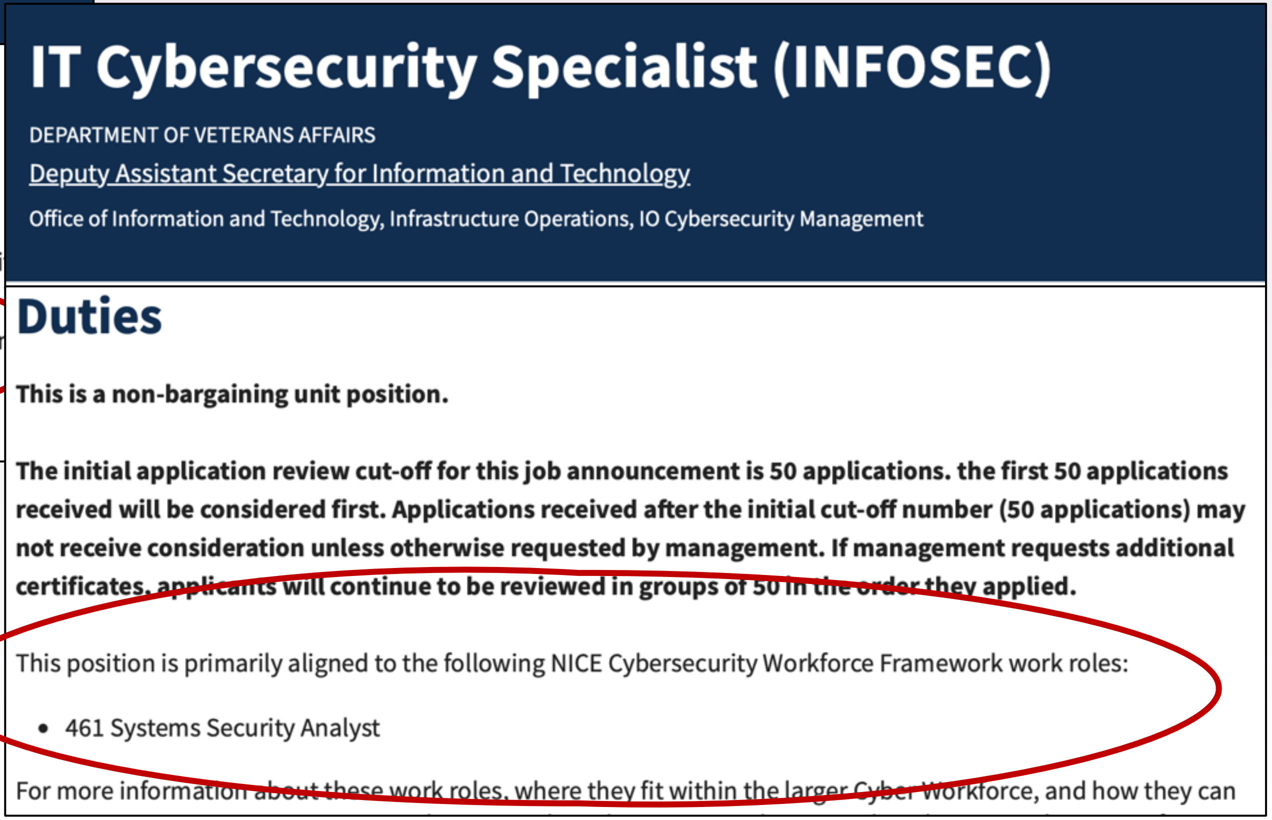
JUDICIAL BRANCH

Administrative Office of the U.S. Courts

IT Security Office, Security Operations Division

judiciary.

8. Documenting and communicating with all internal and external stakeholders to ensure relevant data is provided for sound decision-making and situational awareness.
9. Understanding attack signatures, tactics, techniques, and procedures associated with advanced threats. .
10. The incumbent of this position must be able to perform the tasks and meet the skills, knowledge and abili described in NIST Special Publication 800-181 National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework for the roles of Cyber Crime Investigator (IN-INV-001) and Cyber Defer Forensics Analyst (IN-FOR-002).



IT Cybersecurity Specialist (INFOSEC)

DEPARTMENT OF VETERANS AFFAIRS

Deputy Assistant Secretary for Information and Technology

Office of Information and Technology, Infrastructure Operations, IO Cybersecurity Management

Duties

This is a non-bargaining unit position.

The initial application review cut-off for this job announcement is 50 applications. the first 50 applications received will be considered first. Applications received after the initial cut-off number (50 applications) may not receive consideration unless otherwise requested by management. If management requests additional certificates, applicants will continue to be reviewed in groups of 50 in the order they applied.

This position is primarily aligned to the following NICE Cybersecurity Workforce Framework work roles:

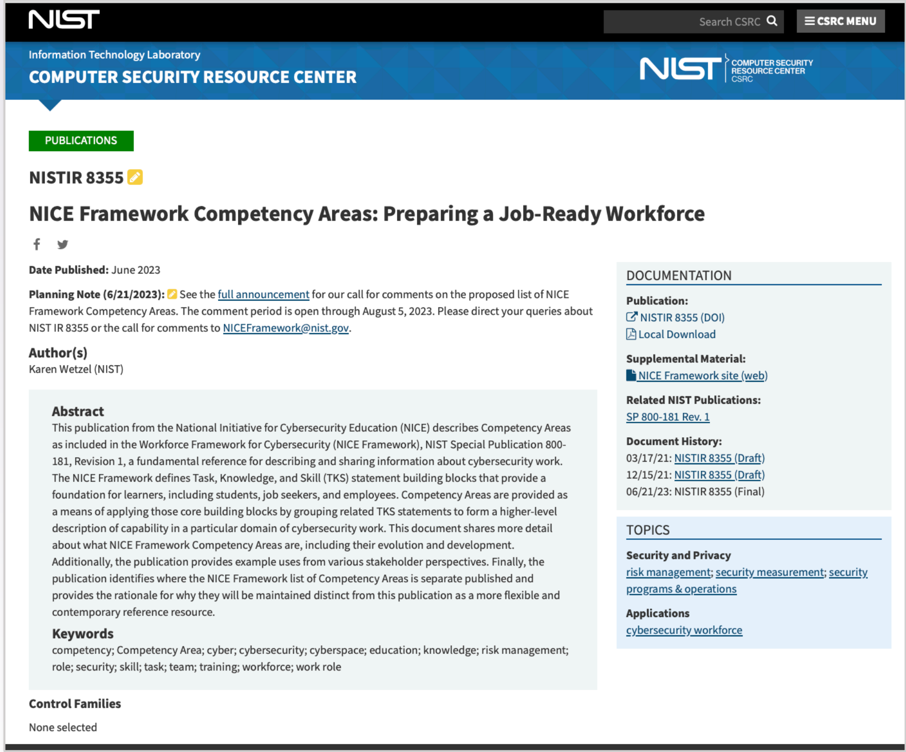
- 461 Systems Security Analyst

For more information about these work roles, where they fit within the larger Cyber Workforce, and how they can

https://cybersecurity.usajobs.gov/job/756222600
https://www.usajobs.gov/job/746332400

NICE Framework Competency Areas: Preparing a Job-Ready Workforce

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


Search CSRC
≡ CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
COMPUTER SECURITY RESOURCE CENTER CSRC
PUBLICATIONS

NISTIR 8355

NICE Framework Competency Areas: Preparing a Job-Ready Workforce

Date Published: June 2023

Planning Note (6/21/2023): See the full announcement for our call for comments on the proposed list of NICE Framework Competency Areas. The comment period is open through August 5, 2023. Please direct your queries about NIST IR 8355 or the call for comments to NICEFramework@nist.gov.

Author(s)
Karen Wetzel (NIST)

Abstract
This publication from the National Initiative for Cybersecurity Education (NICE) describes Competency Areas as included in the Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800-181, Revision 1, a fundamental reference for describing and sharing information about cybersecurity work. The NICE Framework defines Task, Knowledge, and Skill (TKS) statement building blocks that provide a foundation for learners, including students, job seekers, and employees. Competency Areas are provided as a means of applying those core building blocks by grouping related TKS statements to form a higher-level description of capability in a particular domain of cybersecurity work. This document shares more detail about what NICE Framework Competency Areas are, including their evolution and development. Additionally, the publication provides example uses from various stakeholder perspectives. Finally, the publication identifies where the NICE Framework list of Competency Areas is separate published and provides the rationale for why they will be maintained distinct from this publication as a more flexible and contemporary reference resource.

Keywords
competency; Competency Area; cyber; cybersecurity; cyberspace; education; knowledge; risk management; role; security; skill; task; team; training; workforce; work role

Control Families

None selected

DOCUMENTATION

Publication:
NISTIR 8355 (DOI)
Local Download

Supplemental Material:
NICE Framework site (web)

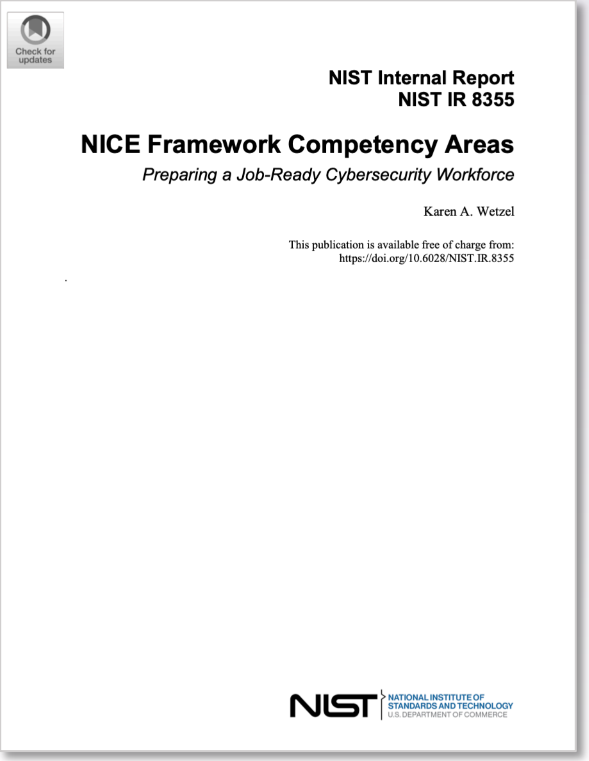
Related NIST Publications:
SP 800-181 Rev. 1

Document History:
03/17/21: NISTIR 8355 (Draft)
12/15/21: NISTIR 8355 (Draft)
06/21/23: NISTIR 8355 (Final)

TOPICS

Security and Privacy
risk management; security measurement; security programs & operations

Applications
cybersecurity workforce



NIST Internal Report
NIST IR 8355

NICE Framework Competency Areas

Preparing a Job-Ready Cybersecurity Workforce

Karen A. Wetzel

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8355

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Resource: NICE Framework Competency Areas (NISTIR 8355)

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 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

NICE Framework Proposed Competency Areas*

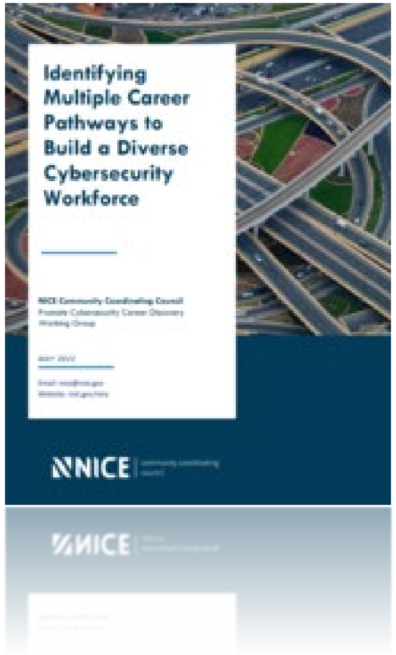
- GROUPINGS OF KNOWLEDGE AND SKILL STATEMENTS
- CORRELATE WITH CAPABILITY TO PERFORM TASKS IN A DOMAIN

1. Access Controls
2. Artificial Intelligence (AI) Security
3. Asset Management
4. Cloud Security
5. Communications Security
6. Cryptography
7. Data Privacy and Security
8. DevSecOps
9. Cyber Resiliency
10. Operation Systems (OS) Security
12. Operational Technology (OT) Security
13. Supply Chain Security

*This slide is based on proposed Competency Areas and expected changes based on comments received. Final adjudication of feedback from public comments is still in process; expected release February 2024

Education and Career Pathways

- **Education Pathways**: Different routes learners follow as they move into, through, and out of an education and training system
- **Career Pathways:** A combination of rigorous and high quality **education, training, and other services** that
  - Aligns with regional industry skill needs
  - Includes education concurrent with and in the same context as workforce preparation activities and training
  - Enables credential achievement at both secondary (e.g., high school diploma) and post-secondary levels
  - Helps individuals enter or advance in an occupation or career



Identifying Multiple Career Pathways to Build a Diverse Cybersecurity Workforce

NICE Community Coordinating Council
Promote Cybersecurity Career Discovery Working Group

MAY 2022

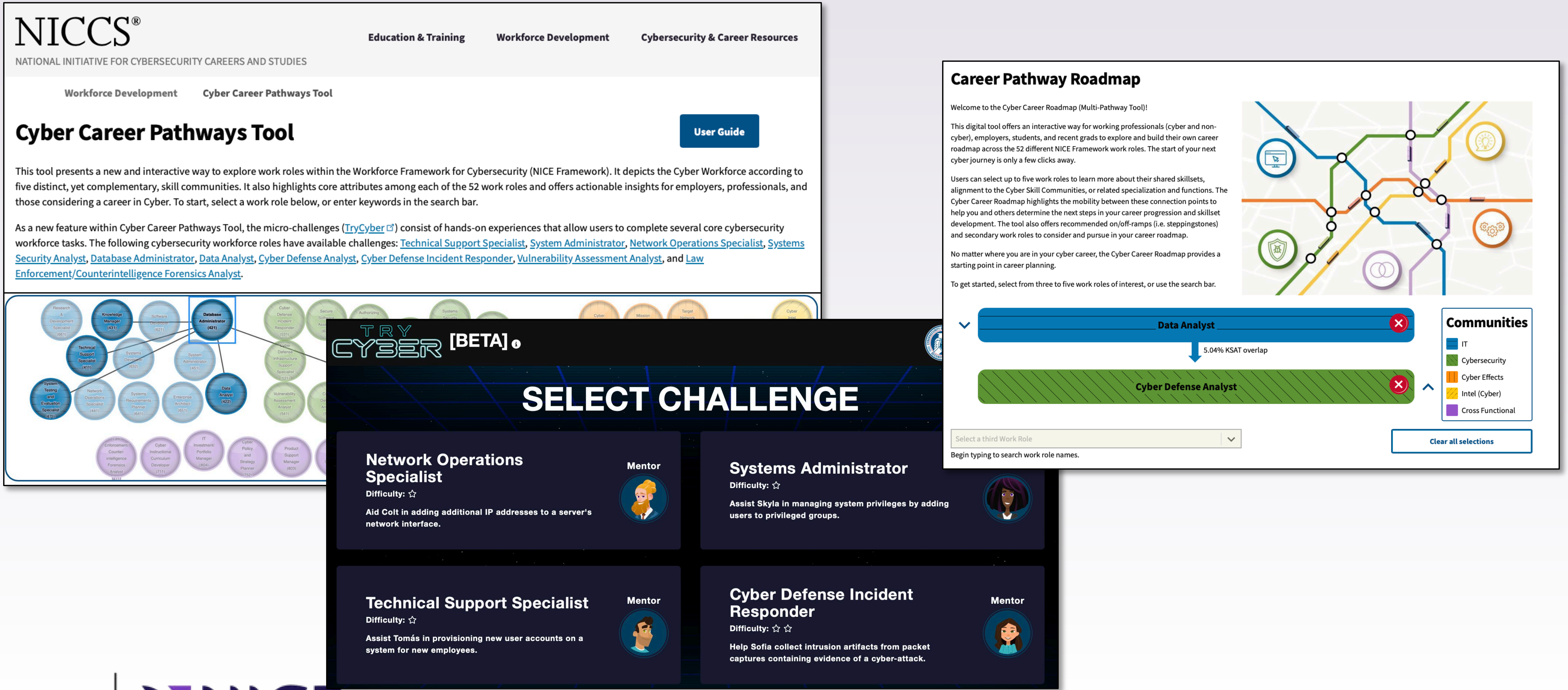
Email: nice@nist.gov
Website: nist.gov/nice

NICE | Community Coordinating Council

Image Source: Original

Resource: NICE Career Pathway Resources

Cybersecurity Career Pathway Tools: NICCS



NICCS®
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

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

As a new feature within Cyber Career Pathways Tool, the micro-challenges (TryCyber) consist of hands-on experiences that allow users to complete several core cybersecurity workforce tasks. The following cybersecurity workforce roles have available challenges: Technical Support Specialist, System Administrator, Network Operations Specialist, Systems Security Analyst, Database Administrator, Data Analyst, Cyber Defense Analyst, Cyber Defense Incident Responder, Vulnerability Assessment Analyst, and Law Enforcement/Counterintelligence Forensics Analyst.

TRY CYBER [BETA]

SELECT CHALLENGE

Network Operations Specialist — Mentor
Difficulty: ☆
Aid Colt in adding additional IP addresses to a server's network interface.

Systems Administrator
Difficulty: ☆
Assist Skyla in managing system privileges by adding users to privileged groups.

Technical Support Specialist — Mentor
Difficulty: ☆
Assist Tomás in provisioning new user accounts on a system for new employees.

Cyber Defense Incident Responder — Mentor
Difficulty: ☆ ☆
Help Sofia collect intrusion artifacts from packet captures containing evidence of a cyber-attack.

Career Pathway Roadmap

Welcome to the Cyber Career Roadmap (Multi-Pathway Tool)!

This digital tool offers an interactive way for working professionals (cyber and non-cyber), employers, students, and recent grads to explore and build their own career roadmap across the 52 different NICE Framework work roles. The start of your next cyber journey is only a few clicks away.

Users can select up to five work roles to learn more about their shared skillsets, alignment to the Cyber Skill Communities, or related specialization and functions. The Cyber Career Roadmap highlights the mobility between these connection points to help you and others determine the next steps in your career progression and skillset development. The tool also offers recommended on/off-ramps (i.e. steppingstones) and secondary work roles to consider and pursue in your career roadmap.

No matter where you are in your cyber career, the Cyber Career Roadmap provides a starting point in career planning.

To get started, select from three to five work roles of interest, or use the search bar.

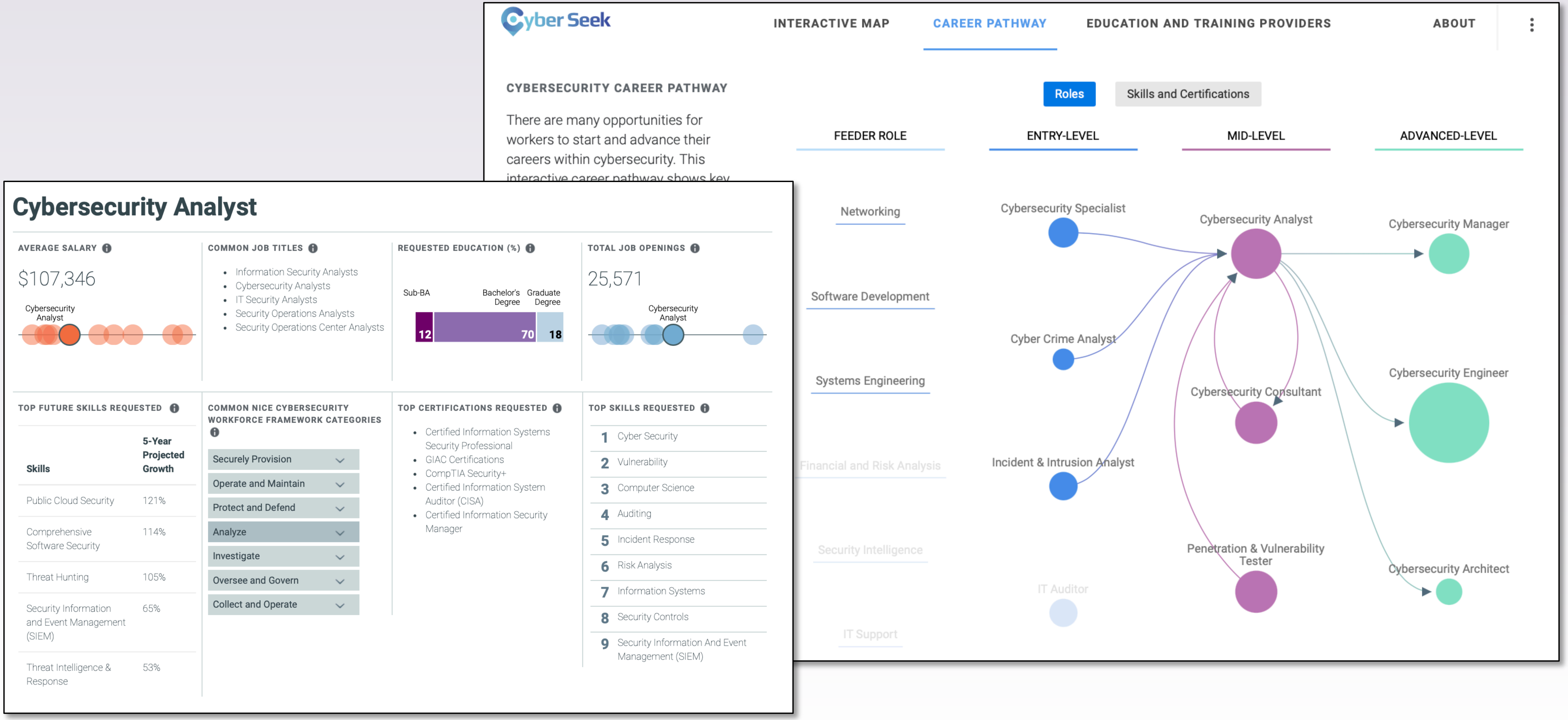
Data Analyst
5.04% KSAT overlap
Cyber Defense Analyst

Communities
- IT
- Cybersecurity
- Cyber Effects
- Intel (Cyber)
- Cross Functional

NIST | NICE

https://niccs.cisa.gov/ https://trycyber.us/

Cybersecurity Career Pathway Tools: CyberSeek



CYBERSECURITY CAREER PATHWAY

There are many opportunities for workers to start and advance their careers within cybersecurity. This interactive career pathway shows key

Cybersecurity Analyst

AVERAGE SALARY

$107,346

COMMON JOB TITLES

- Information Security Analysts
- Cybersecurity Analysts
- IT Security Analysts
- Security Operations Analysts
- Security Operations Center Analysts

REQUESTED EDUCATION (%)

TOTAL JOB OPENINGS

25,571

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 Vulnerability
3 Computer Science
4 Auditing
5 Incident Response
6 Risk Analysis
7 Information Systems
8 Security Controls
9 Security Information And Event Management (SIEM)

NIST NICE

www.cyberseek.org

https://pxhere.com/en/photo/1575607

Evolving to Meet Current and Future Needs

- **Updated TKS Statements**
  - Updated Knowledge and Skill Statements
  - Task Statements (Open for Comment)
  - Full release: February 2024
- **Work Role Updates & New Roles**
  - Insider Threat Analysis (Released for Comment)
  - OT Cybersecurity Engineering (Forthcoming)
  - Under consideration:
    - Cybersecurity Awareness
    - Product Security
    - Cybersecurity Risk Analysis
    - Cybercrime Prosecution
    - And more…
- **Competency Area Development**
- **Proficiency Scale**

1

Equip every American with foundational cyber skills

2

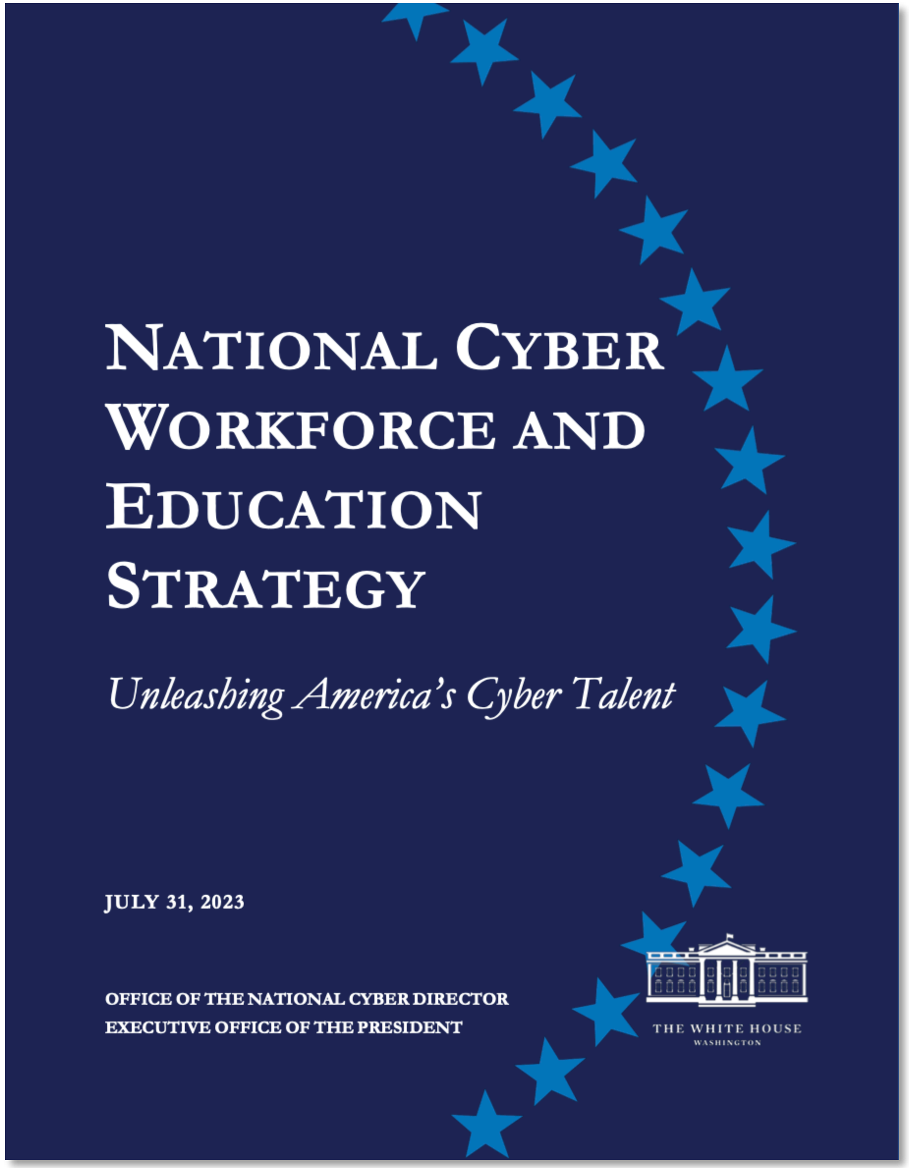
Transform cyber education

3

Expand and enhance America's cyber workforce

4

Strengthen the Federal cyber workforce



National Cyber Workforce and Education Strategy

Unleashing America's Cyber Talent

JULY 31, 2023

OFFICE OF THE NATIONAL CYBER DIRECTOR
EXECUTIVE OFFICE OF THE PRESIDENT

THE WHITE HOUSE
WASHINGTON

Resource: www.whitehouse.gov/cyberworkforce

Engage with NICE

- NICE Framework Users Group
- NICE Interagency Coordinating Council
- NICE Community Coordinating Council
- NICE Working Groups & Project Teams
- NICE Communities of Interest
- Career Ambassadors
- Calls for Comments, Workshops, Webinars, Conferences

»» **Resource**: NICE Communities

NIST | NICE

Image source: shutterstock.com

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, Educators, and Learners
- TKS, Competency Area Authoring Guides
- Employers Guide to Developing Job Descriptions
- Planned: Proficiency Levels, updated data spreadsheet, Competency Area development, new Work Roles, usage guides, and more

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.

NIST | NICE