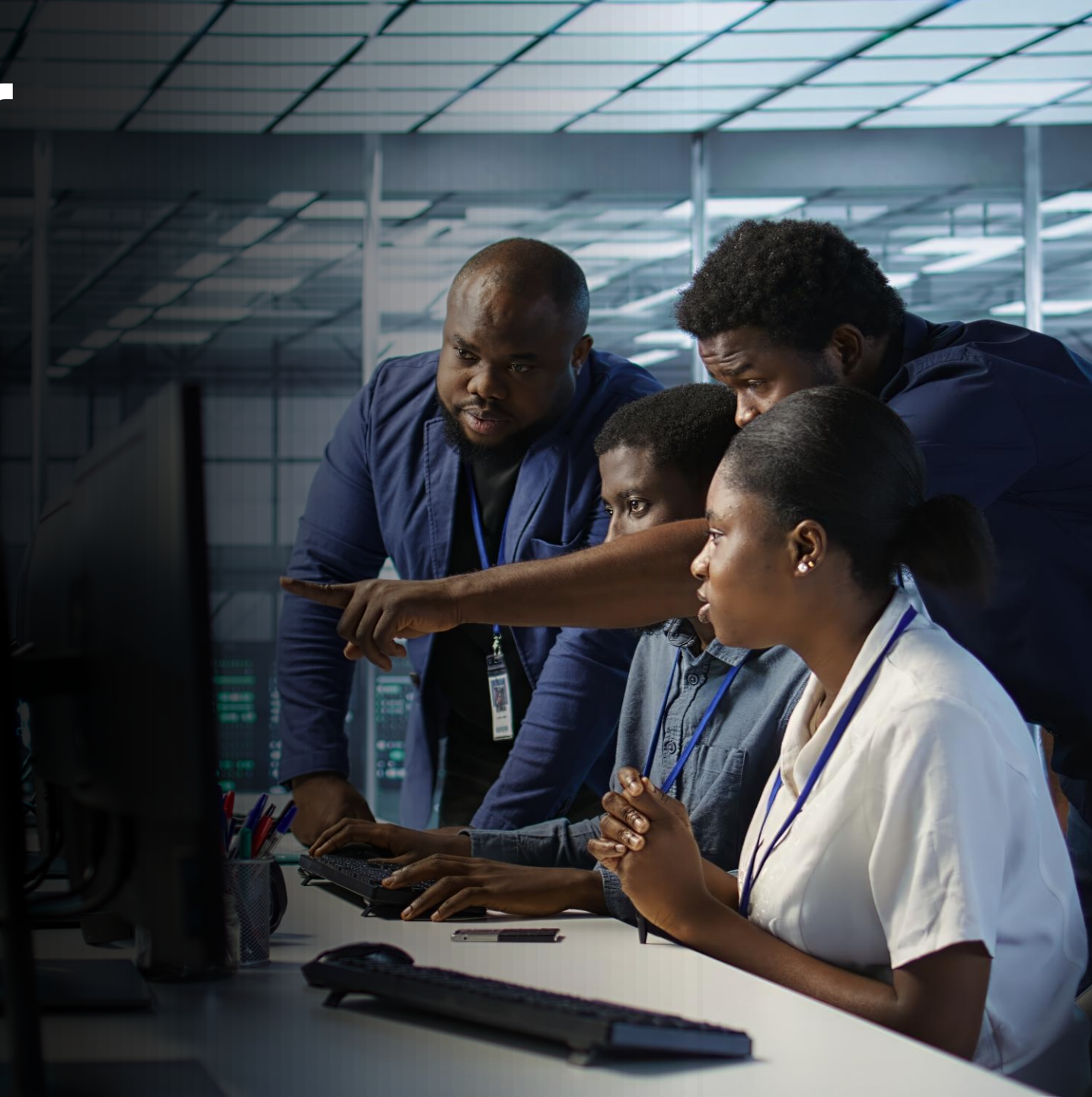


explorecyber

Cybersecurity, AI, and You

Kristine Christensen, Ph.D.

Director, Faculty Development &
Professor, Computer Information Systems &
Automation & Engineering Technology
PI, ExploreCyber.org
Moraine Valley Community College





About NCyTE

- National Science Foundation (NSF) funded center for cybersecurity education for more than 10 years
- One of 27 NSF funded Advanced Technical Educational (ATE) Centers
- Latest funding: \$7.5M over five years
- Supporting nearly 70 distinct activities
- **Mission:** Increase the quantity and quality of the cybersecurity workforce throughout the nation

NCYTE CENTER
National Cybersecurity Training & Education Center

<https://www.ncyte.net/>

About NCyTE – Four Principal Goals

Goal 1:

Expand cybersecurity education pathways and program diversity to meet the nation's cybersecurity needs of tomorrow.

Goal 2:

Develop and deploy leading edge cybersecurity curriculum.

Goal 3:

Cultivate industry engagement and career opportunities.

Goal 4:

Disseminate efforts to improve current and future directions of cybersecurity education in the U.S.

<https://www.ncyte.net/>



Cybersecurity Workforce Gap

- **Severe Workforce Shortage:** There are an estimated 4 million unfilled cybersecurity jobs globally, with over 500,000 vacancies in the U.S. alone.
- **Rising Demand:** Cybersecurity job growth is projected to increase **35% from 2021 to 2031**, significantly outpacing the average job growth rate (Bureau of Labor Statistics).
- **Increasing Cyber Threats:** The rapid rise of cybercrime, ransomware, and nation-state attacks has heightened the need for a skilled cybersecurity workforce.
- **Shortage of Qualified Professionals:** Many job applicants lack the necessary hands-on skills, certifications, and specialized training required to meet industry demands.
- **Continues to Hold National Attention:** White House Office of the National Cyber Director (ONCD)

Where Do You Fit In?

- You do **not** need to be a cybersecurity major.
- Cyber roles exist for:
 - Computer science students
 - Data / AI students
 - Engineering students
 - All students!
- Cybersecurity is a **layer on top of what you already know**





Some Things I Want You to Know About Cybersecurity

Correct misconceptions

Cybersecurity isn't too technical and doesn't happen dispel the notion that cybersecurity is too technical

Understand the value of cybersecurity certifications

Providing information of key industry certifications (e.g., CompTIA Security+) and insights into the relevance of certifications at different career stages

Become aware of extracurricular activities

Create awareness on competitions, clubs, internships, apprenticeships, and other volunteer opportunities in cybersecurity that will build cybersecurity skills

Build confidence and self-efficacy

Enhance their knowledge and confidence in advising on cybersecurity careers and skills, simplifying and explaining roles to inspire career exploration



What is cybersecurity?

- protecting information, information systems, networks, devices, and data from unauthorized access and digital attacks.

Cybersecurity professionals:

- are responsible for ensuring **confidentiality, integrity, and availability** of systems and information.
- Every app you build needs security
- Every AI model you train has risk
- Every system you design can be exploited

CIA Triad

Cybersecurity protects:

- **Confidentiality**
Protecting information from unauthorized access
- **Integrity**
Ensuring data accuracy and preventing unauthorized modification
- **Availability**
Ensuring systems and data are accessible when needed





Cybersecurity & You

What You're Learning	Cybersecurity Connection
Programming	Secure coding, vulnerabilities
Databases	Data protection, breaches
AI/ML	Model security, bias, attacks
Networking	Threat detection
Systems	Hardening and defense

Cybersecurity

Computer Science

Computer / Electrical Engineering

Business

Social Sciences

Cyber Operations

Cyber Forensics

Cyber Engineering

Cyber IT

Cyber Risk Mgmt.

Cyber Human Factors

Cyber Public Policy

Cyber Legal & Ethics

Technical

Non-Technical

Interdisciplinary Demand for Cybersecurity Skills

- **Cyber touches every field:** healthcare, law enforcement, agriculture, education, and manufacturing
- **Smart devices + data = growing risk across all sectors**
- **Professionals need cyber awareness,** not just cyber specialists
- Employers want **job-ready workers** with both technical and domain-specific knowledge



NICE Cybersecurity Work Role Categories




The NICE Framework includes the following components:

Work Role Categories: A high-level grouping of common cybersecurity functions.

Work Roles: A grouping of work for which someone is responsible or accountable. Please note, Work Roles are not synonymous with job titles or occupations.

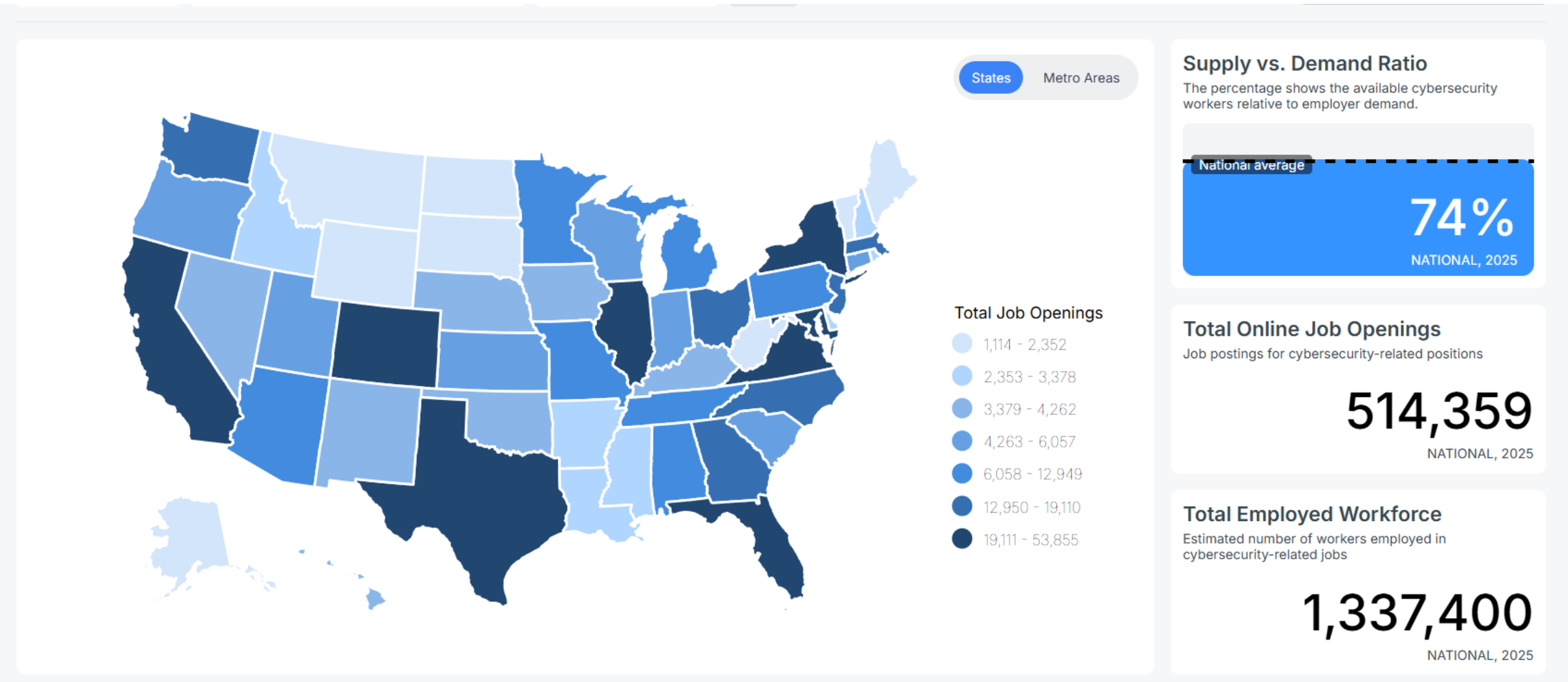
TKS Statements: A set of discrete building blocks that describe the work to be done (in the form of Tasks) and what is required to perform that work (through Knowledge and Skills).

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

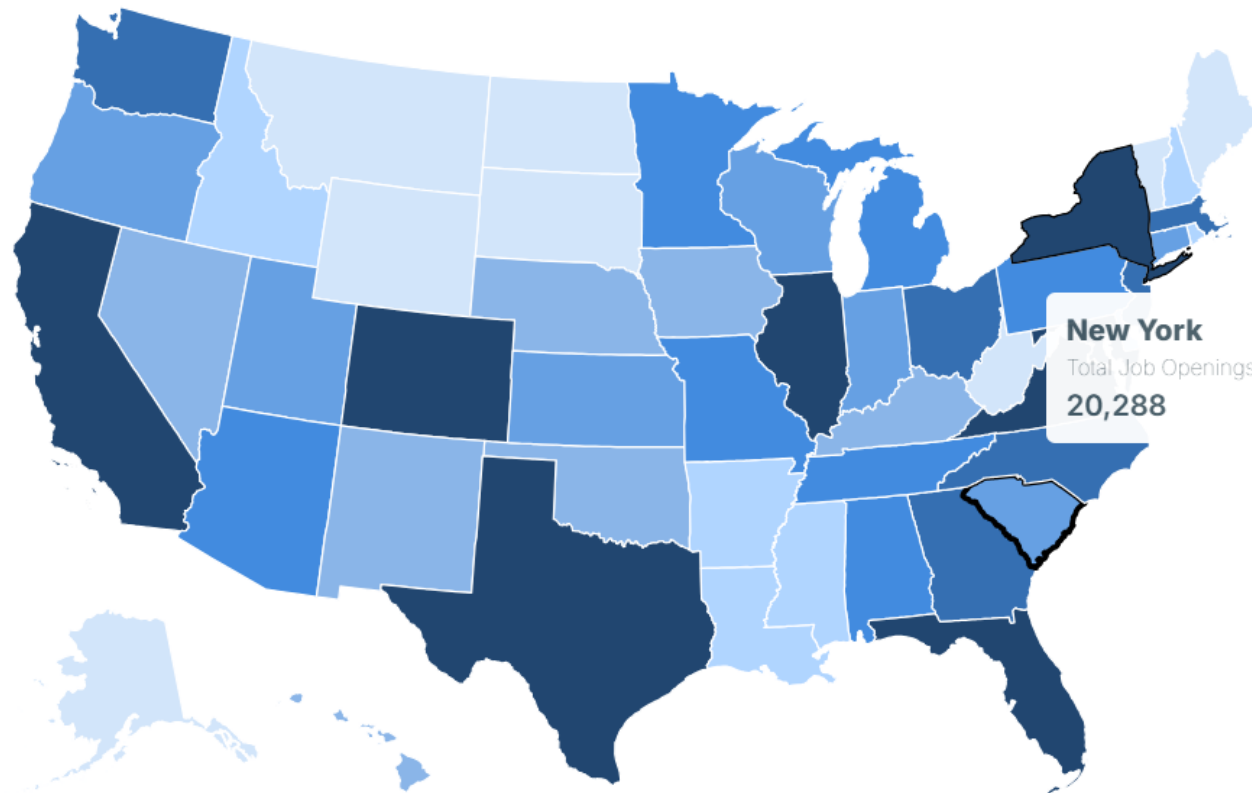
	Oversight and Governance (OG) Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.	^
	Design and Development (DD) Conducts research, conceptualizes, designs, develops, and tests secure technology systems, including on perimeter and cloud-based networks.	^
	Implementation and Operation (IO) Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security.	^
	Protection and Defense (PD) Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.	^
	Investigation (IN) Conducts national cybersecurity and cybercrime investigations, including the collection, management, and analysis of digital evidence.	^

Source: <https://niccs.cisa.gov/tools/nice-framework>

CyberSeek Heat Map & Career Pathways



CyberSeek Heat Map: South Carolina



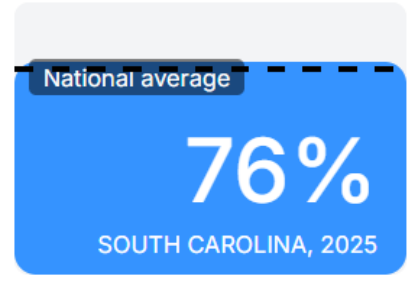
New York
Total Job Openings
20,288

States Metro Areas

- Total Job Openings
- 1,114 - 2,352
 - 2,353 - 3,378
 - 3,379 - 4,262
 - 4,263 - 6,057
 - 6,058 - 12,949
 - 12,950 - 19,110
 - 19,111 - 53,855

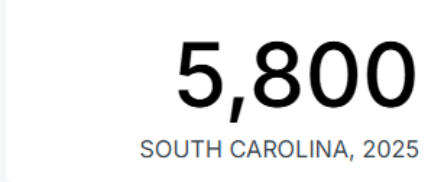
Supply vs. Demand Ratio

The percentage shows the available cybersecurity workers relative to employer demand.



Total Online Job Openings

Job postings for cybersecurity-related positions



CyberSeek Career Pathways

Feeder Roles

Financial and Risk Analysis

IT Support

Networking

Security Intelligence

Software Development

Systems Engineering

Starting-Level

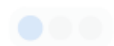
Cybersecurity Specialist



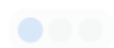
Cyber Crime Analyst



Incident & Intrusion Analyst



IT Auditor



Mid-Level

Cybersecurity Analyst



Cybersecurity Consultant



Penetration & Vulnerability Tester



Advanced-Level

Cybersecurity Manager



Cybersecurity Engineer



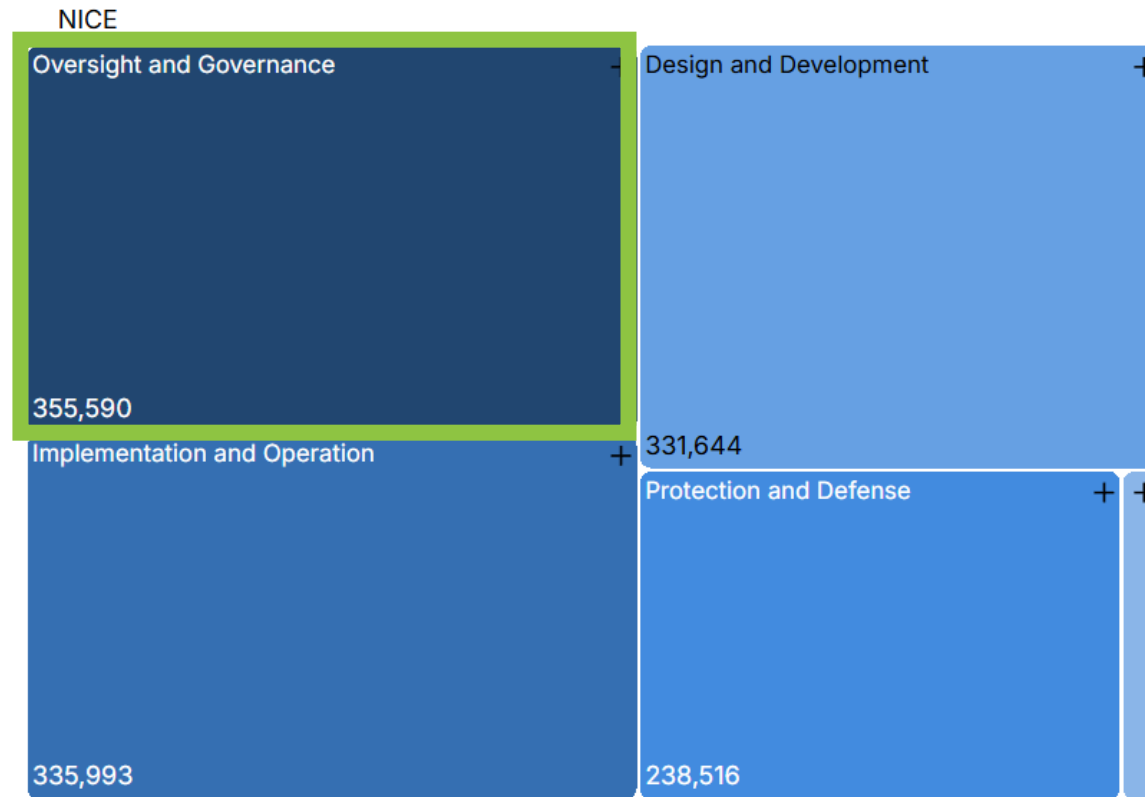
Cybersecurity Architect



CyberSeek: Highest Job Vacancies by Category

Job Openings by NICE Cybersecurity Workforce Framework Category

Shows the number of cybersecurity job openings between May 2023 through April 2024 mapping to each NICE Cybersecurity Workforce Framework category.



Supply vs. Demand Ratio

The percentage shows the available cybersecurity workers relative to employer demand.

National average

74%

NATIONAL, 2025

Total Online Job Openings

Job postings for cybersecurity-related positions

514,359

NATIONAL, 2025

Total Employed Workforce

Estimated number of workers employed in cybersecurity-related jobs

1,337,400

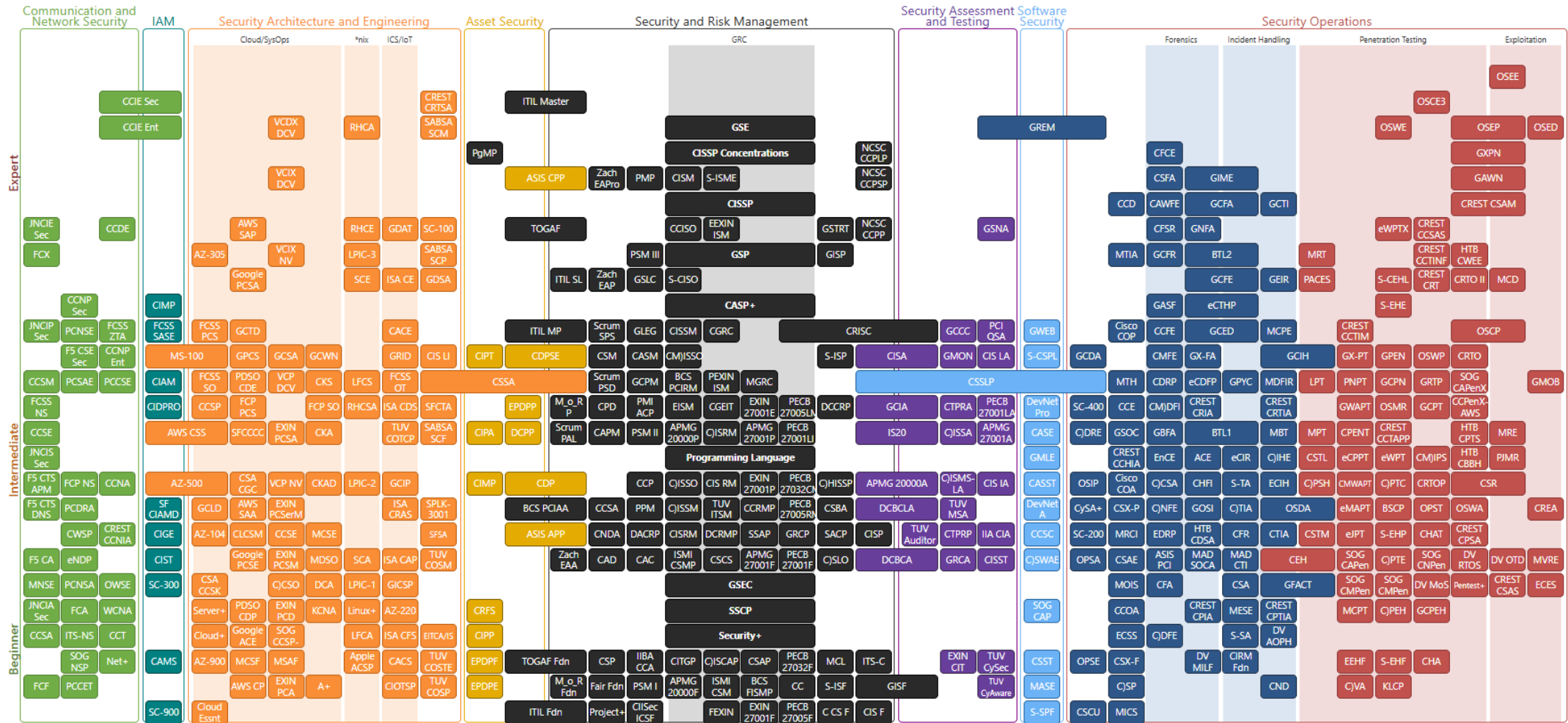
NATIONAL, 2025

<https://www.cyberseek.org/>

OPM Cyber Workforce Dashboard



Industry Certification Roadmap



481 certifications listed | July 2024

DoW Cyber Workforce Framework (DCWF)

The seven Cyberspace Workforce Elements are:



Cybersecurity Career Areas & Student Interests

Career Area	What They Do	Ideal For Students Who...
Security Analyst	Monitor systems and respond to incidents	Like problem-solving, puzzles, and patterns
Penetration Tester (Ethical Hacker)	Test systems to find vulnerabilities	Enjoy challenges, games, or “catching the bad guy”
Cyber Forensics Specialist	Investigate breaches and gather digital evidence	Like criminal justice or investigative work
Network Defender	Protect systems from attacks and maintain security tools	Are detail-oriented and technical
Risk Analyst / Policy Specialist	Evaluate risks, write policies, ensure compliance	Enjoy writing, communication, or law
Security Engineer / Architect	Design and build secure systems	Like designing, planning, and building
Cyber Educator / Trainer	Teach or train others in cybersecurity	Like mentoring and helping people learn

ExploreCyber — Personality & Work Role Matching

Discover cybersecurity careers aligned to how you prefer to think, learn, and work.

Get Started in Two Easy Steps

1. **Learn your personality type.** Visit 16Personalities.com and take the free assessment:

Free Personality Test (16Personalities)

Prefer a faster check? Try our Quick Personality Explorer:

Quick Personality Explorer (High School)

Quick Personality Explorer (Adult)

2. **Use your type to match work roles.** With your four-letter type (e.g., *INTJ*, *ESFP*), explore cybersecurity roles using either the NICE (NIST) or DCWF (DoD) framework.

Tip: Use these results as a conversation starter, not a final answer. Combine this tool with real experiences such as student clubs, workshops, or internships to explore your best fit.

Explore Your Match Using the NICE and DCWF Framework

NICE and DCWF share a common language for describing cyber work. The NICE Framework (NIST) standardizes how roles are described across education, industry, and government. The DoD Cyber Workforce Framework (DCWF) builds on NICE for defense needs, adding DoD-specific role codes, qualification levels, and certification guidance. Together, they help you map roles from civilian to defense contexts.

NICE Framework

What it is: The NICE Workforce Framework for Cybersecurity (NICE Framework), developed by NIST, is a nationally focused resource that establishes a common lexicon for describing cybersecurity work and workers across public, private, and academic sectors.

DCWF Framework

What it is: The DoD Cyber Workforce Framework (DCWF) is a standardized framework developed by the Department of Defense to categorize and describe the full spectrum of cyber workforce roles, building upon the NICE Framework but tailored for DoD-specific needs.

Personality Exploration & Work Role Matcher

<https://i.explorecyber.org/>

Emerging Cybersecurity Fields

- **AI and Cybersecurity** – protecting AI systems and data
- **Industrial / Critical Infrastructure Security** – protecting factories, energy grids, and hospitals
- **Privacy and Compliance** – working with laws and data protection (great crossover for students interested in law or policy)
- **Cloud Security** – securing data stored in the cloud
- **Space Cybersecurity** – securing satellites and aerospace systems

Cal Poly California
Cybersecurity Institute (CII)
Space Grand Challenge



<https://sgc-sandbox.cacyber.net/>

National Centers of Academic Excellence (CAE) in Cybersecurity



CAE
IN CYBERSECURITY
COMMUNITY

CAE-C Designations

- Are regionally accredited institutions offering cybersecurity-related degrees, including majors, minors, and/or certificates at the Associates, Bachelor's and graduate levels.
- The Institution must demonstrate it:
 - Engages in significant community involvement, academic activities, and instructional practices in cybersecurity
 - Has one or more Program(s) of Study (POS) meeting the requirements set forth by the National Security Agency (NSA)
 - Promotes and supports quality academic programs of higher learning that help produce the nation's cyber workforce.

CAE Community Map



CAE INSTITUTION MAP

CAE Institution Map

Use the filters below to find institutions that match your needs.

Institution Name

- CAE Designation -

- State -

Distance (mi) Zip Code

GenCyber Host ⓘ

Scholarship for Service ⓘ

Cyber Service Academy ⓘ

APPLY RESET

The map displays a large number of blue circular markers representing CAE institutions across the United States and parts of Canada. The markers are densely clustered in the Northeast corridor, particularly around New York City and Washington D.C., and are more sparsely distributed in the West and Midwest. The map interface includes a sidebar with filter options and a main map area with navigation controls.

Cybersecurity Scholarship Programs & Extracurricular Activities



Cybersecurity Scholarship Opportunities

- **CyberCorps: Scholarship for Service**

<http://sfs.opm.gov>



- **Department of War Cyber Service Academy**
<https://www.cyber.mil/dod-workforce-innovation-directorate/csa/>

FOREIGN AFFAIRS **IT**
Fellowship

- **Foreign Affairs Information Technology Fellowship**

<https://www.faitfellowship.org/>

- **Diplomatic Technology Officer Career:**

<https://www.faitfellowship.org/dto-career/>

Cybersecurity Activities & Competitions



<https://www.xpcyber.com/>



<https://trycyber.us>

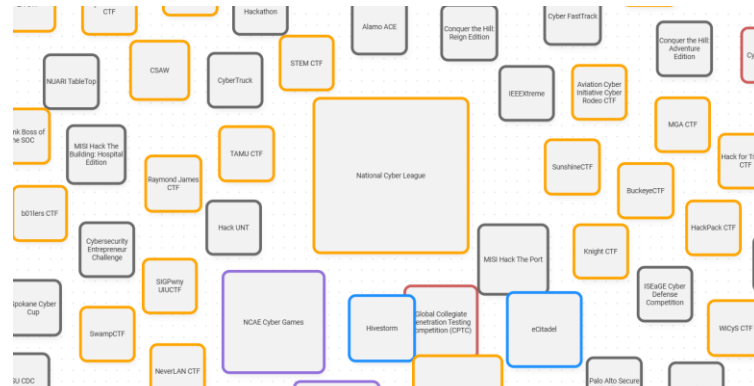


<https://nationalcyberleague.org>



NCAE
CYBER GAMES
PLAY | LEARN | PROTECT

<https://www.ncaecybergames.org/>



<https://cyber-atlas.caecommunity.org/>

Extracurricular Activities & Competitions



The screenshot shows the Cisco Academy course page for 'Introduction to Cybersecurity'. The course is part of the 'Career Path - Junior Cybersecurity Analyst'. It is a self-paced online course available in English (English) and has 8,331,872 enrolled students. The course is free, takes 6 hours, and is beginner-level. It includes 7 labs and is self-paced. The page also lists available languages: العربية, Bahasa Indonesia, 中文(简体), Deutsch, English, Español, Français, Ελληνικά, Italiano, 日本語, 한국어, Nederlands, Polski, Português, Română, ไทย, Türkçe, Український.

Introduction to Cybersecurity
This course is part of the **Career Path - Junior Cybersecurity Analyst**

Explore the exciting field of cybersecurity and why cybersecurity is a future-proof career.

Self-Paced Online
Learn online at your own pace

Instructor-Led
Learn with an academy

English (English)

Get Started With Self-Paced
8,331,872 already enrolled

AVAILABLE LANGUAGES
العربية, Bahasa Indonesia, 中文(简体), Deutsch, English, Español, Français, Ελληνικά, Italiano, 日本語, 한국어, Nederlands, Polski, Português, Română, ไทย, Türkçe, Український

FREE **6 HOURS** **BEGINNER**

7 LABS **SELF-PACED**

<https://www.netacad.com/>



The WiCyS logo features a stylized shield with a power button symbol in the center, colored in purple, green, and blue. To the right of the shield, the text 'women in CYBERSECURITY' is written in a sans-serif font, with 'WiCyS' in a larger, colorful font below it.

women in
CYBERSECURITY
WiCyS

<https://www.wicys.org/>



<https://www.cisa.gov/careers/work-rolescyber-and-it-interns>

Microsoft Learn: Free Courses with Badging



Describe the concepts of cybersecurity

2 hr 17 min • Learning Path • 0 of 6 modules completed

4500 XP

At a glance

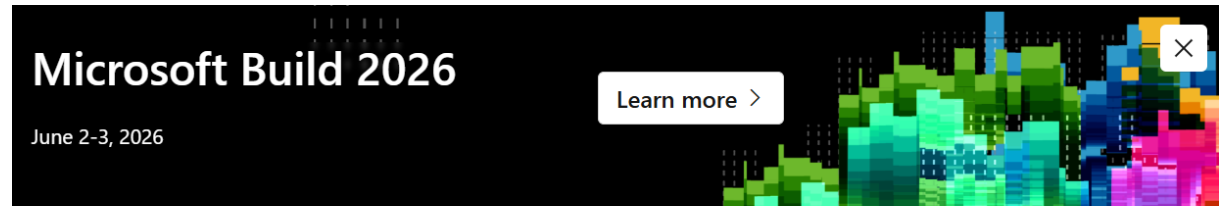
Level
Beginner

Product
Azure, Microsoft 365

Role
Business Owner, Business User, Student

Subject
Security

Knowing the fundamentals of cybersecurity is a first step toward protecting against cyberthreats. In this learning path you will learn about cybersecurity concepts and ways to protect yourself and your business from cyberattacks.



Learn | Documentation ▾ Training & Labs ▾ Q&A ▾ Topics ▾ Search [Sign in](#)

AI | AI documentation ▾ AI training ▾ More ▾

[Open Microsoft Foundry Portal](#)

[Get started with Azure](#)

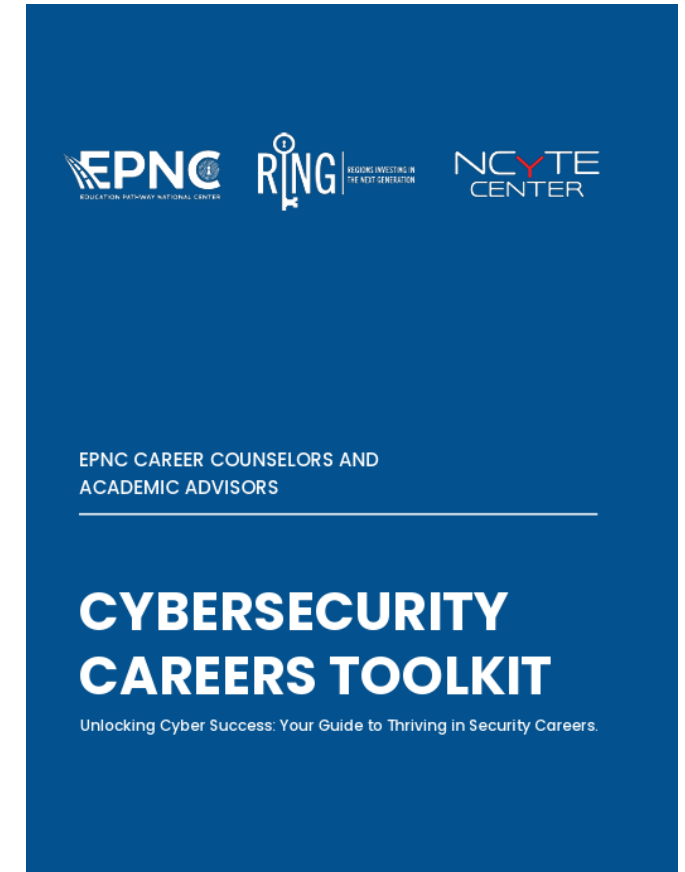
MICROSOFT LEARN AI learning hub

Accelerate your AI learning with resources tailored for technical and business roles to support AI skill development for individuals and organizations. Find curated AI training for any level of AI fluency, like designing and customizing agents at scale with Microsoft Foundry, advancing your expertise in managing AI workloads with Microsoft 365 Copilot, unleashing your creativity and productivity with Microsoft Copilot, and more.

<https://learn.microsoft.com/en-us/training/paths/describe-basic-concepts-of-cybersecurity/>

Creating Awareness: Cybersecurity Careers Toolkit

- **Career Guide** – Supports counselors and advisors in guiding students into cybersecurity careers.
- **Education Pathways** – Covers degrees, certifications, and scholarships.
- **Career Tools** – Features NICE & DCWF Frameworks, CyberSeek, and CYBER.ORG resources.
- **Hands-on Experience** – Highlights competitions and workforce readiness programs.

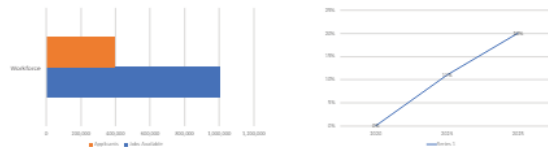


Creating Awareness: Cybersecurity Career Pathways Toolkit

DEFINING AND UNDERSTANDING THE CYBERSECURITY WORKFORCE

The cybersecurity occupation is still a relatively new profession. However, this profession has grown exponentially over the last 20 years.

More than one million cybersecurity jobs will be available by 2023, but less than 400,000 cybersecurity professionals will be trained by then. Cybersecurity is an ever-growing industry. It is projected to grow by 11% in 2023 and by 20% in 2025. This is a fast-paced career with a median salary of \$81,000.



The shortage of qualified professionals is largely due to the rapidly growth for new professionals as well as the growing cyber threats. By prioritizing and promoting cybersecurity careers, career and academic advisors help the nation and the local communities mitigate the risk of data breaches, financial losses, and interruptions to critical business operations and supply chains.



<https://www.youtube.com/watch?v=wV2mlS3aNE>

ACTIVITY 1 – EXPLORING CYBERSECURITY CAREERS

Activity one provides an opportunity for participants to explore Cybersecurity Careers using several of the Cybersecurity Careers Toolkit for career Counselors and Academic Advisors. The activity will introduce three toolkit resources:

1. Workforce Framework for Cybersecurity (NICE Framework)
2. Cyber Careers Pathways Tools
3. Cybersecurity for Students (NICCS Portal)

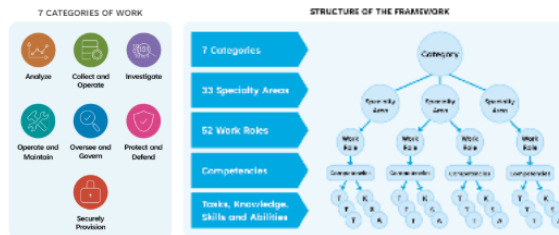
EXPLORING CYBERSECURITY CAREERS

PART 1 - GO TO THE FOLLOWING URL:

<http://niccs.cisa.gov/workforce-development/nice-framework>

The National Initiative for Cybersecurity Education (NICE) is a framework that assist employers, government agencies and academy in developing a robust pipeline of cybersecurity professionals. The framework organizes the cybersecurity workforce into an understandable framework. The framework consists of:

- Categories and Specialization Areas or Work;
- Specific Work Roles
- Associates Task, Knowledge, Skills, and Abilities



COMPETENCY EDUCATION - RESOURCES

Workforce Framework for Cybersecurity (NICE Framework)

The NICE Framework establishes a common lexicon to describe cybersecurity work and workers regardless of where or for whom the work is performed.

niccs.cisa.gov/workforce-development/nice-framework



Cyber Career Pathways Tool

Interactively explore the NICE Cybersecurity Workforce Framework according to five distinct skill communities and attributes for 52 work roles.

niccs.cisa.gov/workforce-development/cyber-career-pathways-tool



Cybersecurity for Students

Find resources and information for cybersecurity students, including education and training opportunities in the field.

niccs.cisa.gov/education-training/cybersecurity-students



CAE Institution Map

The CAE Institution map showcases the locations of CAEs designated by the NSA and the DHS in the field of cybersecurity education.

caecommunity.org/cae-map



Cyber.org - Career Profiles

Cyber.org provides an overview of various cyber career profiles, offering information and insights into different roles within the cybersecurity field.

cyber.org/career-exploration/cyber-career-profiles



Cyber Seek - Heat Map and Pathways

Cyber Seek provides interactive tools and data to explore cybersecurity job demand, skills, and career pathways in the United States.

www.cyberseek.org/index.html



Our Website



<https://www.explorecyber.org/>



We're just getting started, and we'd love to collaborate!

Explore Cyber is an evolving initiative, and our team is actively developing new materials, workshops, and resources to support cybersecurity career awareness.

Check back often as we expand our Toolkit, add interactive content, and share updates about our progress.

Our Mission

To expand cybersecurity career awareness, empower educators, and build pathways that connect students to high-demand cyber roles across every industry.

Our Goals

- **Inspire Interest:** Spark curiosity in cybersecurity through engaging, approachable activities.
- **Empower Educators:** Provide tools aligned with the NICE Workforce Framework to help advisors and teachers confidently discuss cyber careers.
- **Broaden Access:** Encourage collaboration across multiple disciplines so students in fields like business, health, engineering, and the arts can see how cybersecurity connects to their future careers.
- **Connect Pathways:** Strengthen bridges between education and industry so students graduate ready for real-world careers.

What We Do

Did You Know?

More than 500,000 cybersecurity positions in the U.S. remain unfilled—and demand is expected to grow by over 30% in the next decade. Yet many students, educators, and career advisors are unaware of the wide range of opportunities this field offers. Explore Cyber helps bridge that gap by providing tools and resources to guide future professionals into cybersecurity careers.

ExploreCyber — Personality & Work Role Matching

Discover cybersecurity careers aligned to how you prefer to think, learn, and work.

Get Started in Two Easy Steps

1. **Learn your personality type.** Visit 16Personalities.com and take the free assessment:

Free Personality Test (16Personalities)

Prefer a faster check? Try our Quick Personality Explorer:

Quick Personality Explorer (High School)

Quick Personality Explorer (Adult)

2. **Use your type to match work roles.** With your four-letter type (e.g., *INTJ*, *ESFP*), explore cybersecurity roles using either the NICE (NIST) or DCWF (DoD) framework.

Tip: Use these results as a conversation starter, not a final answer. Combine this tool with real experiences such as student clubs, workshops, or internships to explore your best fit.

Explore Your Match Using the NICE and DCWF Framework

NICE and DCWF share a common language for describing cyber work. The NICE Framework (NIST) standardizes how roles are described across education, industry, and government. The DoD Cyber Workforce Framework (DCWF) builds on NICE for defense needs, adding DoD-specific role codes, qualification levels, and certification guidance. Together, they help you map roles from civilian to defense contexts.

NICE Framework

What it is: The NICE Workforce Framework for Cybersecurity (NICE Framework), developed by NIST, is a nationally focused resource that establishes a common lexicon for describing cybersecurity work and workers across public, private, and academic sectors.

DCWF Framework

What it is: The DoD Cyber Workforce Framework (DCWF) is a standardized framework developed by the Department of Defense to categorize and describe the full spectrum of cyber workforce roles, building upon the NICE Framework but tailored for DoD-specific needs.

Personality Exploration & Work Role Matcher

<https://i.explorecyber.org/>



First Steps You Can Take

- Join a cybersecurity club or event
- Try a CTF
- Take one online module (Microsoft Learn fits perfectly here)
- Talk to a faculty member or advisor
- Explore one career pathway

NCyTE Community College Faculty Fellowship

Fellowship Information: <https://www.ncyte.net/career-seekers/career-seeker-resources/fellowship-program>



explore cyber



This material is based upon work supported by the National Science Foundation under Grant No. 2500740. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation

Healthcare and Public Health Sector

- Protecting Lives and Medical Data
- **Critical Assets:** Hospitals, Acute Care Facilities, Pharmaceutical companies, Medical Device Managers, Emergency Medical Services

Sector Composition:

- 6,000+ hospitals in the United States
- 250,000+ healthcare facilities including clinics and nursing homes
- \$4.3 trillion annual healthcare spending
- 18% of US GDP represented by healthcare



Common Attacks:

- **Ransomware** - Increasingly targets hospitals for maximum impact
- **Data theft** - PHI valuable on black markets
- **Medical device compromises** - Insulin pumps, pacemakers, imaging systems
- **Supply chain attacks** - Compromised medical software and devices

Healthcare and Public Health Sector

Cybersecurity Challenges:

- **Legacy Systems:** Medical devices designed for longevity, not security.
- **Availability Requirements:** Cannot take critical systems offline for updates.
- **Interoperability Needs:** Systems must communicate across organizations.
- **Regulatory Complexity:** HIPAA, FDA, and state requirements.
- **Resource Constraints:** Tight budgets limit security investments.

Case Study:

Yale New Haven Health Data Breach

- **What happened:** Sophisticated hackers gained unauthorized access to a network server, exposing demographic data for approximately **5.6 million patients:** names, DOBs, addresses, race/ethnicity, and medical record numbers
- **Why it matters:** 5.56 million patients affected: **largest healthcare breach of 2025**
- **Data compromised:** Names, addresses, SSNs, medical record numbers. *Protected Data:* Medical records, financial information, treatment details
- **Key takeaway:** Lack of basic safeguards (e.g., segmentation, encryption) not only jeopardizes patient data but invites regulatory and legal consequences, plus severe reputational damage.



Case Study:

Ascension Health Ransomware Incident (2024)

- **What happened:** Ransomware attack by Black Basta (Russian), on May 8, 2024, crippled Ascension's digital systems across 140 hospitals, forcing manual paper-based operations – ambulance diversions and delayed care.
- **Cause:** **Employee** accidentally downloaded a malicious file thinking it was legitimate
- **Why it matters:** Electronic Health Records (EHRs) were inaccessible. Critical diagnostics (e.g., stroke CT scans) are delayed by hours, disrupting surgeries, pharmacy, radiology, and emergency services.
- **Data compromised:** Medical records, Social Security numbers, credit card info, insurance
- **Key takeaways:** Cybersecurity failures can **threaten lives**, not just data. Demonstrates how employee error can trigger massive operational disruption and the critical importance of cybersecurity training in healthcare



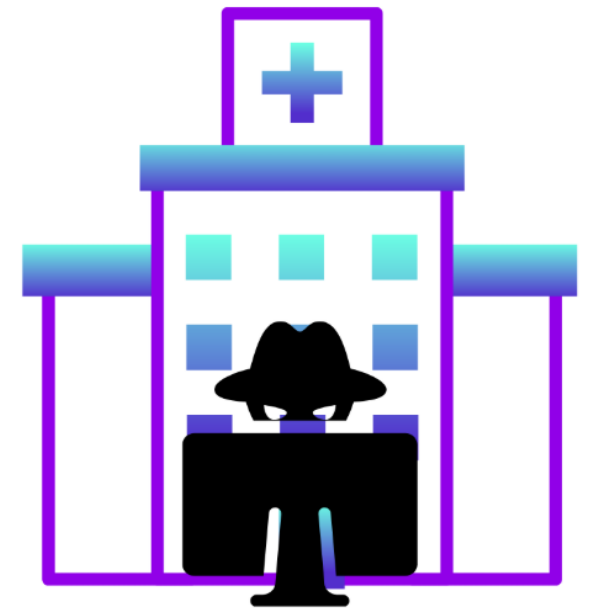
Resources for Health Science Classes

- **HHS 405(d) Program – Health Industry Cybersecurity Practices (HICP):**
offers free downloadable playbooks, threat scenarios, and best practices
<https://405d.hhs.gov>
- **Health Sector Cybersecurity Coordination Center (HC3):**
Alerts, sector threat briefs, and trend analysis (e.g., ransomware, phishing, zero-days)
<https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html>
- **Health-ISAC Threat Intelligence Reports:**
<https://h-isac.org>

Interactives for Health Science Classes

- **Defend the Hospital (Incident Response)**
<https://cyberskillslive.com/activity/defend-the-hospital/>
- **HackableHospital (Offensive):**
<https://www.hackablehospital.com/>
- **Digital Care Hub (Leadership & Consequence Management Focused):**
<https://www.digitalcarehub.co.uk/digital-skills-and-training/cyber-game/>

HackableHospital



Our Website



<https://www.explore cyber.org/>



We're just getting started, and we'd love to collaborate!

Explore Cyber is an evolving initiative, and our team is actively developing new materials, workshops, and resources to support cybersecurity career awareness.

Check back often as we expand our Toolkit, add interactive content, and share updates about our progress.

Our Mission

To expand cybersecurity career awareness, empower educators, and build pathways that connect students to high-demand cyber roles across every industry.

Our Goals

- **Inspire Interest:** Spark curiosity in cybersecurity through engaging, approachable activities.
- **Empower Educators:** Provide tools aligned with the NICE Workforce Framework to help advisors and teachers confidently discuss cyber careers.
- **Broaden Access:** Encourage collaboration across multiple disciplines so students in fields like business, health, engineering, and the arts can see how cybersecurity connects to their future careers.
- **Connect Pathways:** Strengthen bridges between education and industry so students graduate ready for real-world careers.

What We Do

Did You Know?

More than 500,000 cybersecurity positions in the U.S. remain unfilled—and demand is expected to grow by over 30% in the next decade. Yet many students, educators, and career advisors are unaware of the wide range of opportunities this field offers. Explore Cyber helps bridge that gap by providing tools and resources to guide future professionals into cybersecurity careers.

explore cyber



This material is based upon work supported by the National Science Foundation under Grant No. 2500740. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation



Thank You!

Let's Connect & Collaborate



Kristine Christensen, Ph.D.

Christensen@morainevalley.edu

Director, Faculty Development &
Professor, Computer Information Systems &
Automation & Engineering Technology
Moraine Valley Community College



This material is based upon work supported by the National Science Foundation under Grant No. 2500740. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation