exploreCyber

CAREER COUNSELORS AND ACADEMIC ADVISORS

CYBERSECURITY CAREERS TOOLKIT

Unlocking Cyber Success: Your Guide to Thriving in Security Careers

ExploreCyber, a Cybersecurity Career Awareness and Exploration Initiative (CCAEI), is funded by the National Science Foundation (NSF) Advanced Technological Education (ATE) Program, Grant #2500740.

TABLE OF

CONTENTS

PART I

INTRODUCTION TO CYBERSECURITY CAREERS

What is Cybersecurity?

Cybersecurity is the art of protecting information, information systems, networks, devices, and data from unauthorized access.

Cybersecurity professionals are like the digital world's police force, safeguarding our virtual valuables. They are also responsible for protecting and maintaining secure and reliable communication (e.g., email, smartphones, tablets).

Imagine how much we depend on technology: from personal devices like phones and laptops to massive online systems in fields such as farming, entertainment, shopping, and banking. Cybersecurity experts are the guardians of this realm. They make sure that private conversations stay private, that online shopping is safe, and that the systems we rely on every day are up and running without a hitch. They work in all sorts of industries — from agriculture, manufacturing, and transportation to healthcare, banking, government services, and national defense.

CYBERSECURITY PRINCIPLES

Cybersecurity professionals are responsible for ensuring three foundational properties — often called the CIA Triad:

- **Confidentiality:** ensuring that information is accessible only to those authorized to access it
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods
- **Availability:** ensuring that authorized users have access to information and systems when needed

Virtually every segment of the economy faces cyber threats, including agriculture, manufacturing, education, entertainment, transportation, retail, medicine, logistics, banking, government services, and more. How much of your daily life relies on technology?

DEFINING AND UNDERSTANDING THE

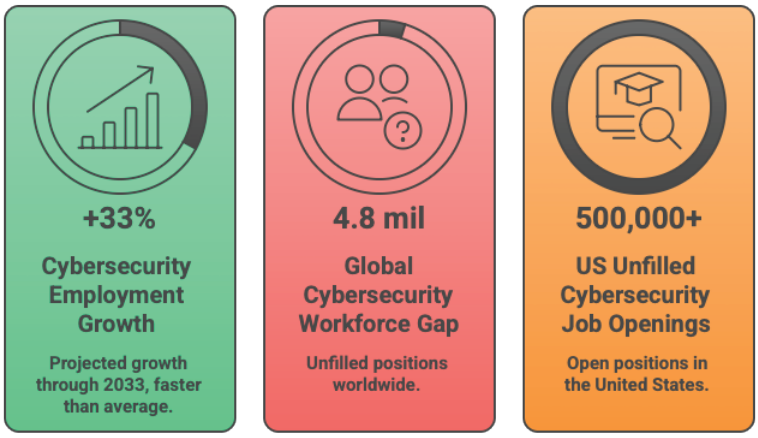
CYBERSECURITY WORKFORCE

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

Key workforce statistics (2024–2026):

- There are approximately 500,000+ unfilled cybersecurity job openings in the United States (CyberSeek, 2025)
- The global cybersecurity workforce gap stands at approximately 4.8 million unfilled positions (ISC2 Cybersecurity Workforce Study, 2024)
- Cybersecurity employment is projected to grow 33% through 2033 — far faster than the average for all occupations (U.S. Bureau of Labor Statistics, 2024)

Cybersecurity Workforce Landscape



- The median annual salary for cybersecurity analysts in the U.S. is approximately $120,000 (BLS, 2024)

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

Explore

Watch this short video on the cybersecurity workforce and career opportunities:
https://www.youtube.com/watch?v=wV2jmlS3oNE

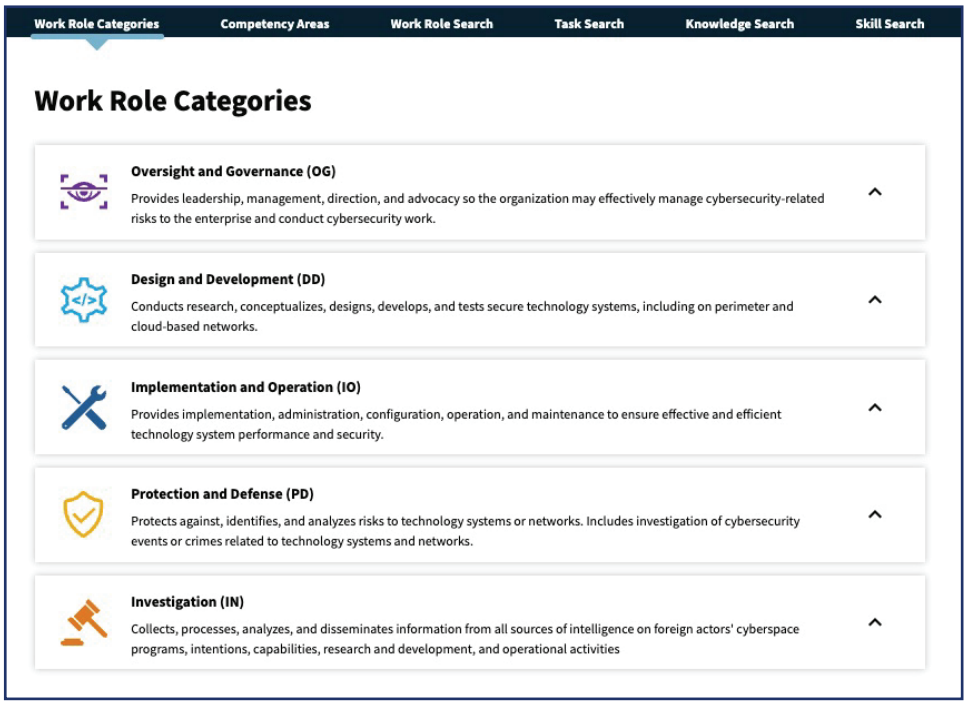
NICE WORKFORCE

WORKFORCE FRAMEWORK 2.0

As the nation focuses on growing the cybersecurity workforce, a framework was developed to clarify the types of work and skills cybersecurity professionals need.

The ***National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (CWF)*** is the foundation for increasing the size and capability of the U.S. cybersecurity workforce.

NIST released CWF 2.0 (NIST SP 800-181r2) in 2023, significantly restructuring and modernizing the original framework. CWF 2.0 establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. It applies across public, private, and academic sectors.



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

Note: CWF 2.0 replaced the previous version's 7-category, 33-specialty-area, 52-work-role structure with a streamlined 5-category, 41-work-role structure. If you have used earlier versions of the framework, note that two categories — Collect and Operate, and Investigate — have been consolidated into the remaining categories. Always reference CWF 2.0 (SP 800-181r2) going forward.

NICE CYBERSECURITY WORKFORCE FRAMEWORK 2.0

FRAMEWORK STRUCTURE

A structured framework defining what cybersecurity professionals do, know, and need to succeed.

CWF 2.0 has three foundational building blocks:

- **Task Statements:** descriptions of work activities directed toward organizational objectives.
- **Knowledge Statements:** descriptions of retrievable concepts a worker needs to know.
- **Skill Statements:** descriptions of a worker's capacity to perform an observable action.

These T-K-S statements are organized into Work Roles (41 total) and grouped into five top-level Work Role Categories:

Category (Abbreviation)	Focus	Example Work Roles
Securely Provision (SP)	Design, build, and implement secure systems and environments	Software Developer, Risk Manager, Systems Requirements Planner, Enterprise Architect
Operate and Maintain (OM)	Provide support, administration, and maintenance of IT/cyber systems	Systems Administrator, Network Operations Specialist, Data Administrator, Tech Support Specialist
Oversee and Govern (OV)	Lead, manage, and advocate cybersecurity missions; develop the workforce	Executive Cyber Leader, Cyber Workforce Developer, Legal Advisor, Privacy Officer, CISO
Protect and Defend (PD)	Identify, analyze, and mitigate threats to systems and networks	Cyber Defense Analyst, Incident Responder, Vulnerability Assessor, Security Architect
Analyze (AN)	Perform highly specialized review and evaluation of cybersecurity information	All-Source Analyst, Threat/Warning Analyst, Exploitation Analyst, Targets Analyst

Full CWF 2.0 interactive tool (all 41 work roles and T-K-S statements): https://niccs.cisa.gov/tools/nice-framework

THE DOD CYBERSPACE WORKFORCE FRAMEWORK

DCWF & DoD 8140

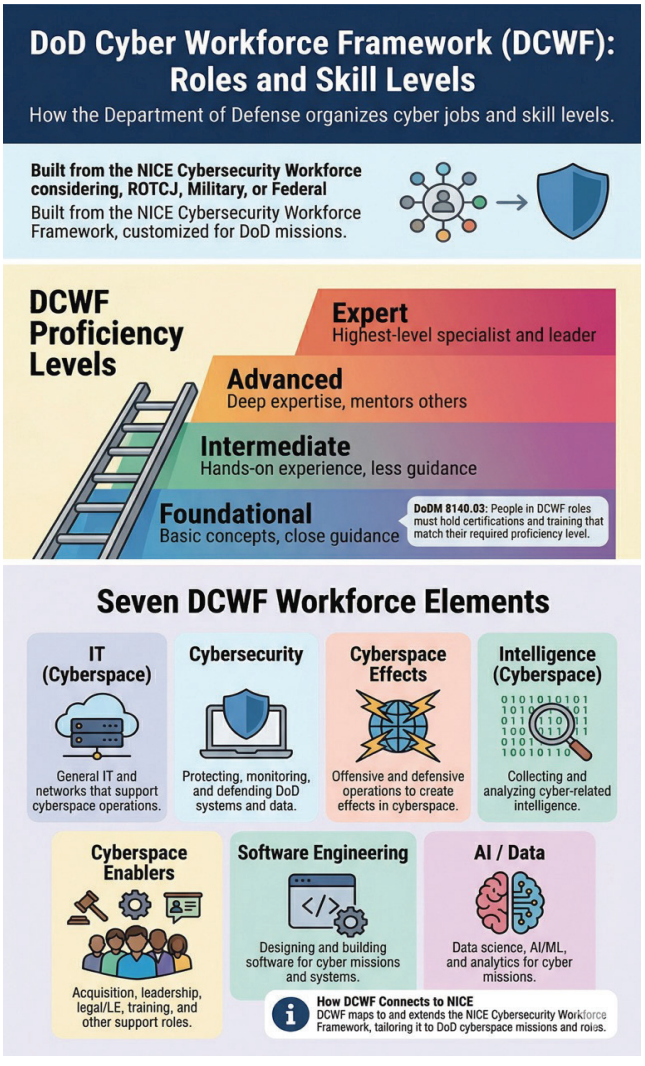
While NICE CWF applies broadly to the national cybersecurity workforce, the Department of Defense operates under the DoD Cyberspace Workforce Framework (DCWF).

Established under DoD Directive 8140.01 and implemented through DoD Manual 8140.03 (2023). Students pursuing careers in defense, military service, federal civilian roles, or government contracting will encounter DCWF requirements directly.

The DCWF maps to and extends the NICE CWF, applying it specifically to DoD cyberspace positions. It assigns proficiency levels, ***Foundational, Intermediate, Advanced, and Expert,*** to each work role. DoDM 8140.03 requires that personnel in designated positions hold certifications meeting baseline qualification requirements for their assigned work role.

The DCWF covers seven workforce elements:

- **IT (Cyberspace):** General IT and network services supporting cyberspace operations.
- **Cybersecurity:** Protecting, monitoring, and defending DoD systems and data.
- **Cyberspace Effects:** Offensive and defensive cyberspace operations to create effects in cyberspace.
- **Intelligence (Cyberspace):** Collecting and analyzing cyber-related intelligence.
- **Cyberspace Enablers:** Acquisition, leadership, legal/LE, training, and other support roles.
- **Software Engineering:** Designing and developing software for cyber missions and systems.
- **AI/Data:** Data science, AI/ML, and related analytics in the cyber mission space.



NATIONAL CYBER WORKFORCE AND EDUCATION STRATEGY

NCWES 2023

In 2023, the White House released the National Cyber Workforce and Education Strategy (NCWES).

The first comprehensive federal strategy for growing and diversifying the cybersecurity workforce. The NCWES emphasizes four priorities:

- **Equipping** every American with foundational cyber skills and digital literacy
- **Transforming** cyber education from K-12 through post-secondary, including CTE and community colleges
- **Expanding** the national cyber workforce through pathways, apprenticeships, and on-ramps
- **Strengthening** the federal cyber workforce through DCWF qualification and improved hiring and retention

Academic advisors and counselors who understand the NCWES can better connect students to federally supported programs, funding streams, and career opportunities aligned with national priorities.

Why This Matters: A National Push for Cyber Talent

The **National Cyber Workforce and Education Strategy (NCWES 2023)** signals a major shift: cybersecurity is no longer a niche field—it's a national priority tied to economic security and national defense.

The strategy focuses on **access and pathways**, not just degrees. That means more opportunities for students through:

- Short-term credentials and certifications
- Paid apprenticeships and internships
- Community college and CTE programs
- Career transitions from non-technical backgrounds

For advisors, this is a key takeaway: **there is no single "right" path into cybersecurity anymore.** Students can enter the field through multiple on-ramps aligned with their interests—technical, analytical, or even policy-focused.

Bottom line: The federal government is actively investing in making cybersecurity careers more accessible, more diverse, and more connected to real workforce needs.

ARTIFICIAL INTELLIGENCE

AI & CYBERSECURITY

Artificial intelligence (AI) is reshaping every corner of the cybersecurity field — simultaneously becoming the most powerful defensive tool available to security teams and one of the most dangerous capabilities in the hands of adversaries.

For students entering the workforce in the next two to five years, understanding the AI-cybersecurity intersection is no longer optional. Advisors who can speak to this intersection help students position themselves at the leading edge of a rapidly transforming job market.

Battle of AI: Sword vs. Shield

Security teams are deploying AI and machine learning (ML) across the full defensive operations lifecycle just as attackers weaponize the same systems to expand the attack surface.

ARTIFICIAL INTELLIGENCE

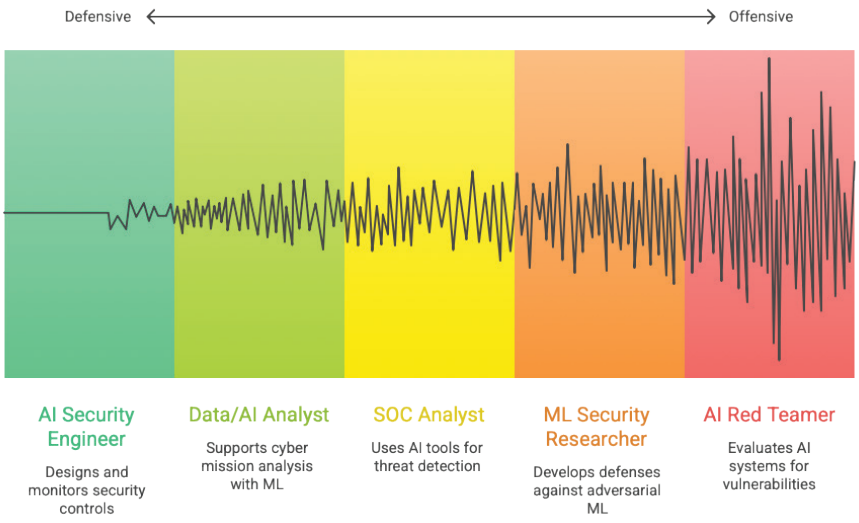
AI & CYBERSECURITY

Emerging Career Roles at the AI-Cybersecurity Intersection

New and evolving work roles at this intersection are among the most rapidly growing and highest-compensated in the field. The DCWF's AI/Data workforce element (DoDM 8140.03) formally recognizes this space within the defense cyber workforce. NICE CWF 2.0 work roles in the Analyze (AN) and Securely Provision (SP) categories are increasingly relevant. Key emerging roles include:

- **AI Security Engineer:** Designs, implements, and monitors security controls specifically for AI/ML systems — including model integrity, access controls for training data, pipeline security, and adversarial robustness testing. Strong demand in cloud, financial services, and defense.
- **Machine Learning Security Researcher:** Studies adversarial ML techniques, develops defenses against model manipulation, and publishes findings. Typically requires graduate-level education (MS or PhD) and combines deep ML expertise with security principles. Common in academic, national lab, and large-tech research contexts.
- **AI Red Teamer:** Evaluates AI systems for security vulnerabilities — including prompt injection, jailbreaks, model extraction, and data leakage. An emerging offensive specialization that combines traditional penetration testing skills with understanding of LLM behavior.
- **Data/AI Analyst (DCWF AI/Data Element):** Applies data science and ML techniques to support cyber mission analysis — including threat intelligence, anomaly detection, and cyber operations support. Directly mapped to the DCWF AI/Data workforce element for students targeting DoD or Intelligence Community careers.
- **SOC Analyst with AI/ Automation Proficiency:** The traditional Tier 1–2 analyst role is evolving to require fluency in AI-assisted tools. Students who understand SOAR platforms, LLM-integrated SIEM, and automated playbooks will have a significant advantage in the near-term job market — these skills are now on most SOC analyst job descriptions.

AI security roles range from defensive to offensive.



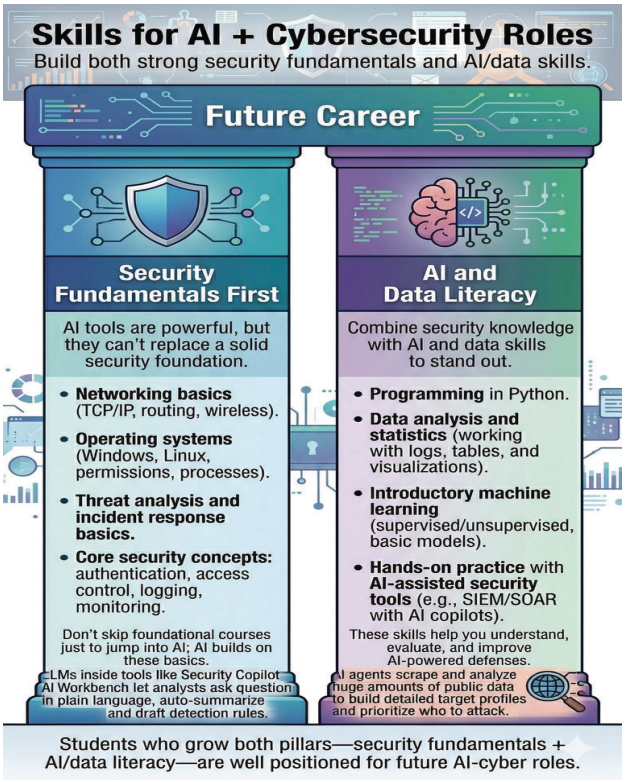
ARTIFICIAL INTELLIGENCE

AI & CYBERSECURITY

Skills Students Should Develop

Students positioning themselves for AI-cybersecurity roles benefit from developing capabilities across two dimensions:

- **Security Fundamentals First:** AI tools augment — ***but do not replace*** — solid grounding in networking, operating systems, threat analysis, and incident response. Students should not skip foundational security education in pursuit of AI specialization.
- **AI and Data Literacy:** Coursework in Python, data analysis, statistics, and introductory ML (e.g., scikit-learn, PyTorch, or equivalent) combined with hands-on experience using AI-assisted security tools provides a strong foundation for differentiation in the job market.



Explore

Have students search for three current cybersecurity analyst job postings on LinkedIn or USAJobs. How many mention AI, machine learning, SOAR, or automation? What specific tools or platforms are listed? Compare findings with classmates. Discuss: How would you build those skills before graduation?

Advisor Tip

When students ask whether AI will 'replace' cybersecurity jobs, reframe the conversation: AI will replace the most repetitive parts of certain roles (Tier 1 alert triage, routine reporting) while increasing demand for analysts who can build, tune, interpret, and investigate AI-generated outputs. The students who learn to work alongside AI tools — rather than compete with them — will be the most employable graduates of this decade.

CYBERSECURITY CAREERS

CYBER CAREER PROFILES

The cybersecurity profession encompasses a vast array of roles — from technicians, engineers, programmers, and scientists to architects, auditors, administrators, executives, investigators, intelligence officers, legal experts, and educators.

Given this diversity, it can be challenging for educators, career counselors, and advisors to assist students in identifying and planning a path to a suitable cybersecurity career. Several organizations offer resources to help.

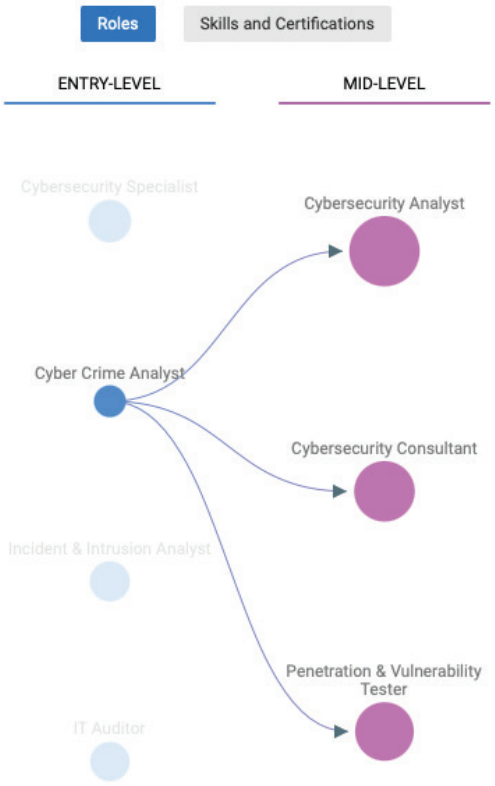
CYBER.ORG is a cybersecurity workforce development organization that targets K-12 students with cyber career awareness, curricular resources, and teacher professional development. One of the many valuable products produced by CYBER.ORG is their "Cyber Career Profiles." These profiles can be downloaded from: https://cyber.org/career-exploration/cyber-career-profiles

Explore

Have students select one of the CYBER.ORG career profiles. Have them identify the type of information provided within the profile. Compare the difference between this tool and the NICE CWF 2.0 data. Website: cyber.org | Also explore cybersecurity careers with 14 virtualized challenges at trycyber.us

CYBERSEEK WEBSITE

CAREER PATHWAYS TOOL

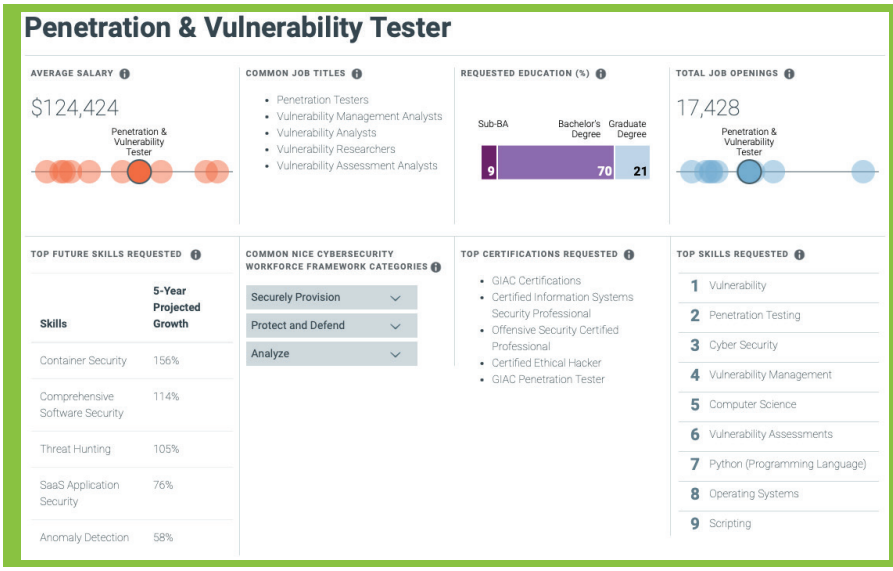


Cyberseek is a joint initiative between the National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce and Lightcast, a leading provider of job market analytics and strategic intelligence.

The ***CyberSeek Pathway Tool*** identifies entry-, mid-, and advanced-level cybersecurity jobs and applies the NICE CWF to help individuals identify the knowledge, skills, and abilities necessary for career advancement.

CyberSeek supports employers, educators, guidance and career counselors, students, current workers, and policy makers.

CyberSeek Career Pathway Tool:
https://www.cyberseek.org/pathway.html



Explore

Have your student lookup the following jobs roles:

- Cybersecurity Specialist
- IT Auditor
- Cyber Crime Analyst
- Cybersecurity Manager

Explore Here!

CYBERSEEK WEBSITE

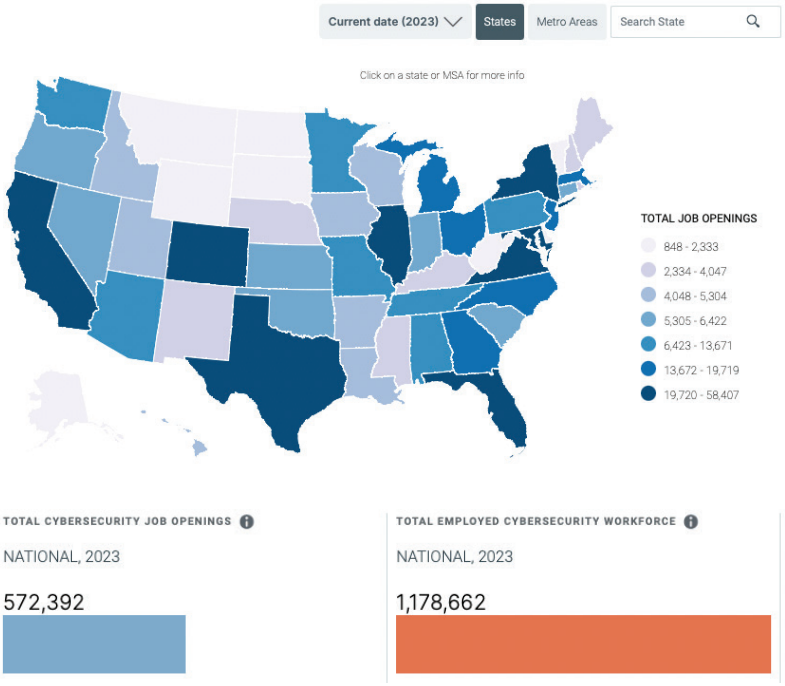
INTERACTIVE HEAT MAP

Have students use the Interactive Cybersecurity Career Map to explore jobs in their states and metropolitan areas.

Prompt them to find the following information:

- Total job openings
- Supply/demand ratio
- Top jobs in the area
- Jobs in each of the five NICE CWF 2.0 categories
- Top credentials requested by employers

https://www.cyberseek.org/heatmap.html



Explore Use the Interactive Cybersecurity Career Map to complete the table below:

State/Metro Area	Total Cyber Job Openings	Top Job Titles	Second Job Title	Top NICE Category	CISSP Holders/ Openings	CISA Holders/ Openings
Illinois						
Chicago						
Virginia						
Los Angeles						

PART II

WHY STUDENTS SHOULD CONSIDER A CAREER IN CYBERSECURITY

WHY CONSIDER A

CAREER IN CYBERSECURITY?

A high-demand, high-impact field with many ways to serve and succeed. Cybersecurity careers are in-demand acress every industry and they need students like you.

OPPORTUNITIES ABOUND

Huge talent shortage and growing demand.

Hundreds of thousands of cyber jobs are unfulfilled in the U.S.

REWARDING COMPENSATION

Entry-level roles often start around $65K, with experienced pros well into the six figures.

Certifications can boost pay even more.

CHALLENGING, NEVER BORING

Fast-changing work that uses critical thinking, teamwork, and constant learning.

No two days look exactly the same.

SERVICE TO OTHERS

Protect people, businesses, schools, and hospitals from digital threats.

Your work keeps data and systems safe.

MANY CAREER PATHS

Hands-on defenders, analysts, policy and governance, educators, and more.

There's a cyber role for every strenght and interest.

PROTECTING THE NATION

Cyber pros help defend critical infrastructure and democratic institutions.

It's a career that is noth impactful and mission-driven.

COMMON STUDENT MISCONCEPTIONS ABOUT

CYBERSECURITY CAREERS

Many students and advisors carry inaccurate mental models of cybersecurity work. Addressing these myths early helps students explore the field with accurate expectations.

Myth: ***Cybersecurity is only for people who love to hack.***

Reality: The field includes policy analysts, risk managers, educators, auditors, legal and compliance specialists, and many other roles that require little to no offensive technical skill. The NICE CWF 2.0 identifies five broad categories — Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, and Analyze — spanning technical, managerial, and governance work.

Myth: You need a Computer Science degree to enter cybersecurity.

Reality: Professionals enter the field from criminal justice, business, political science, education, and the military. Many entry-level roles value certifications (e.g., CompTIA Security+, Google Cybersecurity Certificate) and demonstrated skills over a specific degree title.

Myth: Cybersecurity is a solitary, anti-social career.

Reality: Most cyber roles require collaboration, communication, and the ability to explain complex risks to non-technical audiences such as executives, board members, legal teams, and end users. Strong writing and presentation skills are frequently cited by employers as in-demand differentiators.

Myth: Cybersecurity is too difficult for average students.

Reality: Entry points exist at every skill level. K-12 CTE pathways, community college programs, and free platforms like TryHackMe and Cybersecurity Career Pathway (CyberSeek) allow students to build skills progressively. Competitions like CyberPatriot are designed for students with no prior experience.

Advisor Tip

When a student says, "cybersecurity isn't for me," invite them to explore which of the five CWF 2.0 categories resonates most. This simple reframe can spark new conversations—often revealing interests in areas like policy, leadership, or education that they hadn't previously connected to cybersecurity.

Ultimately, a career in cybersecurity offers students the opportunity to continuously learn and grow, earn a strong income, and make a meaningful impact—both in people's lives and in protecting the security of their communities and country.

PART III

UNDERSTANDING ACADEMIC CREDENTIALS

PURPOSE OF

ACADEMIC CREDENTIALS

Academic credentials serve as evidence that a student completed education and/or training in a specific field, earned college credit, and developed necessary workforce competencies to qualify for entry-level employment.

Many colleges group certificates within college majors or minors. Majors are primary fields of study; minors are secondary concentrations. There are five main categories of academic credentials, commonly known as academic certificates or degrees. College certificates have gained popularity over time. These short-term programs — requiring 12 to 60 college credits — focus on specific skills in demanding fields such as cybersecurity. Certificates can be stackable, allowing students to start with basic certificates and progress to more advanced certificates, ultimately leading to a full college degree.

Technical Certificate Programs

Technical certificates are short- to long-term programs that focus on specific occupational skills and are designed to prepare students for immediate employment or advancement in a particular field. These programs are often "stackable," meaning the credits earned can apply toward a longer-term technical certificate or an associate degree if students choose to continue their education.

Admission Requirements

Typical admission requirements for technical certificate programs include:

- High school diploma, GED, or ability to benefit (requirements vary by program)
- Program-specific prerequisites, such as placement scores or prior coursework, for some technical fields
- Completion of the institution's application process and submission of any required documentation

Program Length and Outcomes

Short-term certificates may be completed in one or two semesters (approximately 15–20 credit hours) and offer a fast path into entry-level roles. Long-term technical certificates usually require 30–45 credit hours over two to three semesters and often include some general education, preparing students for more advanced or higher-paying positions. Many technical certificate programs are developed in partnership with local employers to ensure that students gain industry-relevant, hands-on skills that align with current workforce needs.

PURPOSE OF

ACADEMIC CREDENTIALS

Associate of Science and Associate of Applied Science Programs

Associate degrees are typically two-year programs offered at community colleges and some four-year institutions, providing foundational education and career-focused preparation. An Associate of Science (AS) degree emphasizes transferable general education and disciplinary coursework and is often designed for students planning to continue into a bachelor's program. An Associate of Applied Science (AAS) degree focuses on applied, technical skills that prepare students to enter the workforce directly in fields such as information technology, health care, or advanced manufacturing.

Admission Requirements

Common admission requirements for AS and AAS programs include:

- High school diploma or equivalent (GED)
- Minimum GPA or placement scores (varies by institution and program)
- Completion of placement testing or submission of standardized test scores, if required
- Submission of application forms, transcripts, and any required supporting documents

Average Cost and Program Structure

Tuition for AS and AAS programs at public community colleges is generally lower than for four-year institutions, making them a more affordable entry point into higher education. Most programs require approximately 60–70 credit hours and can be completed in two years of full-time study; part-time enrollment can extend completion time to three or more years. AS programs include a larger share of transferable general education courses, while AAS programs devote more credits to hands-on, technical coursework aligned with specific careers.

PURPOSE OF

ACADEMIC CREDENTIALS

Bachelor's Degree Programs

A bachelor's degree is a four-year program typically offered at universities and colleges, providing in-depth knowledge and specialization in various fields of study. Types of bachelor's degrees include: Bachelor of Arts (BA), Bachelor of Science (BS), Bachelor of Fine Arts (BFA), Bachelor of Applied Science (BAS), Bachelor of Business Administration (BBA), Bachelor of Engineering (BEng), and Bachelor of Computer Science (BCS). These programs open extensive career opportunities and serve as a foundation for advanced education.

Admission Requirements

Common admission requirements for bachelor's degree programs include:

- High school diploma or equivalent (GED)
- Minimum GPA requirements (varies by institution and program competitiveness)
- SAT or ACT scores (many institutions have moved to test-optional policies — verify with the specific school)
- Submission of application forms, transcripts, and required supporting documents
- Letters of recommendation and personal statement (for competitive programs)

Average Cost and Enrollment Options

In 2023–2024, average annual tuition for public in-state students was approximately $11,260, while public out-of-state averaged $29,150 (College Board, 2024). Private nonprofit institutions averaged $41,540 annually. Financial aid, scholarships, and work-study programs can significantly reduce actual costs. Most full-time students complete a bachelor's degree in four years (approximately 120 credit hours). Part-time enrollment is also common, particularly among students who work while studying — extending completion time to five or more years.

PURPOSE OF

ACADEMIC CREDENTIALS

Master's Degree Programs

A master's degree is an advanced level of education following completion of a bachelor's degree. It provides in-depth knowledge, specialization, and advanced skills in a specific field. Types include: Master of Arts (MA), Master of Science (MS), Master of Business Administration (MBA), Master of Education (MEd), Master of Engineering (MEng), Master of Fine Arts (MFA), Master of Public Health (MPH), and Master of Social Work (MSW).

Master's programs typically cost $10,000 to $40,000 per year in tuition, depending on institution and field. Financial aid, employer tuition assistance, and graduate assistantships can help offset costs. Full-time programs typically take one to two years; part-time programs extend to two to four years. A master's degree can unlock senior technical, management, and policy roles and is increasingly expected for security architecture and CISO positions.

Advanced Degrees: Doctoral Programs (PhD)

A doctoral degree — commonly a PhD (Doctor of Philosophy) — is the highest level of education in most fields. Doctoral programs are rigorous and research-focused, preparing students for advanced scholarly work and significant contributions to their field. Types include: Doctor of Philosophy (PhD), Doctor of Business Administration (DBA), Doctor of Education (EdD), and Doctor of Engineering (EngD).

Doctoral programs at research universities often provide funding through stipends, teaching or research assistantships, or fellowships that cover tuition and provide a living allowance. Completion typically requires three to seven years of full-time study. Doctoral degrees open doors to academic positions, senior research roles, industry leadership, and influential government or policy positions.

PURPOSE OF

ACADEMIC CREDENTIALS

Degrees and Lifetime Earning Potential

Having a college degree greatly improves your chances of finding a job and earning more over a lifetime. Individuals with a bachelor's degree face only half the likelihood of unemployment compared to those with only a high school diploma, and they accumulate, on average, an additional $1.2 million in lifetime earnings. Public university graduates — particularly from state schools — show strong economic advancement relative to cost of attendance.

In the cybersecurity field specifically, earning potential increases substantially at each credential level:

Credential Level	Typical Starting Salary	Notes
Associate Degree / Certificate	$50,000–$65,000	Entry-level IT support, help desk, junior analyst roles
Bachelor's Degree	$65,000–$90,000	Cybersecurity analyst, network security, entry GRC roles
Bachelor's + Certifications	$80,000–$110,000	Mid-level analyst, security engineer, compliance specialist
Master's Degree	$95,000–$135,000	Senior analyst, security architect, manager roles
PhD / Doctorate	$110,000–$175,000+	Research, executive, senior federal/academic positions

Explore Find at least four academic credentials related to cybersecurity that interest you. Record the information in the table below:

Institution	Degree/Certificate	Subject Area	Years to Complete

PART IV

CYBERSECURITY MAJORS

TYPES OR MAJORS OF ACADEMIC

CYBERSECURITY PROGRAMS

Multiple academic disciplines provide viable pathways into cybersecurity careers. The right program depends on the student's target role, existing strengths, and institutional offerings. Below are common degree types and how they align with cybersecurity career paths.

Major / Program	Core Focus	Well-Suited For
Cybersecurity / Information Assurance	Purpose-built security curriculum; policy, defense, forensics, risk management	Broad cyber roles; federal and DoD careers; NICE CWF 2.0 alignment; NCAE-C designated programs
Computer Science (CS)	Programming, algorithms, systems, software engineering foundations	Secure software development; security research; malware analysis; cloud security engineering
Information Technology (IT)	Practical systems administration, networking, helpdesk, infrastructure management	Network security; systems admin; SOC analyst; entry-level IT/security roles
Information Systems (IS) / MIS	Business context plus technology; governance, audit, and management focus	GRC analyst; IT audit; compliance; security management; healthcare IT security
Computer Engineering	Hardware, embedded systems, firmware, networking architecture	IoT security; hardware security; industrial control systems (ICS/SCADA); embedded systems
Criminal Justice / Digital Forensics	Investigation, legal framework, chain of custody, evidence handling	Digital forensics; cyber law enforcement; incident response; insider threat analysis
Mathematics / Statistics	Cryptography, data analysis, probability, algorithm development	Cryptographer; data scientist in security; malware analyst; intelligence analysis
Political Science / Public Policy	Policy, regulation, international affairs, risk governance, legislative processes	Cyber policy analyst; DHS/NSC/DOS roles; think tanks; congressional staff; CISO in government

MINORS, CONCENTRATIONS, AND STACKABLE CREDENTIALS

OTHER QUALIFICATIONS

Students in non-cyber majors can substantially strengthen their cybersecurity qualifications by adding a cybersecurity minor, concentration, or certificate alongside their primary degree.

Common high-value additions include: cybersecurity minor, network security certificate, data privacy certificate, digital forensics concentration, and cloud security certificate. Ask whether your institution's cybersecurity courses are mapped to NICE CWF 2.0 competency areas.

Many community colleges offer stackable certificate pathways — beginning with short-term certificates in specific areas (e.g., Network Defense, Security Operations) that can be combined and credited toward an AAS or AS degree, which can then articulate to a four-year program.

Connecting Your Major to CWF 2.0 Work Roles

A practical exercise for advisors and students: identify two or three target work roles in CWF 2.0 and reverse-engineer the coursework, skills, and experiences needed. Use the NICE CWF interactive tool at niccs.cisa.gov to browse all 41 work roles by category. Look at the Task and Knowledge statements for your target roles and ask:

"Which courses in our program address these T-K-S statements?"

Explore

Have your student identify a cybersecurity career they find interesting. Look it up in the NICE CWF 2.0 interactive tool (niccs.cisa.gov/workforce-framework). What category does it fall in? What are the top five Knowledge and Skill statements for that work role? Which courses at your institution address those statements?

PART V

CYBERSECURITY INDUSTRY CREDENTIALS

CYBERSECURITY

INDUSTRY CERTIFICATIONS

In the fast-paced world of cybersecurity, having the right education credentials is just the starting point.

What truly sets professionals apart are industry certifications — official stamps of approval earned by passing exams and demonstrating real-world competency.

For newcomers cutting their teeth in technology, certifications mark a universal baseline of knowledge, skills, and familiarity with specific tools. For seasoned professionals, they are a way to demonstrate prowess in specific technical domains. From an organization's perspective, certifications are proof that their workforce can defend digital assets against threats. When it comes to cybersecurity certification bodies, some credentials carry more weight in the industry. Aim for top-tier credentials from well-established bodies as a foundation, then specialize.

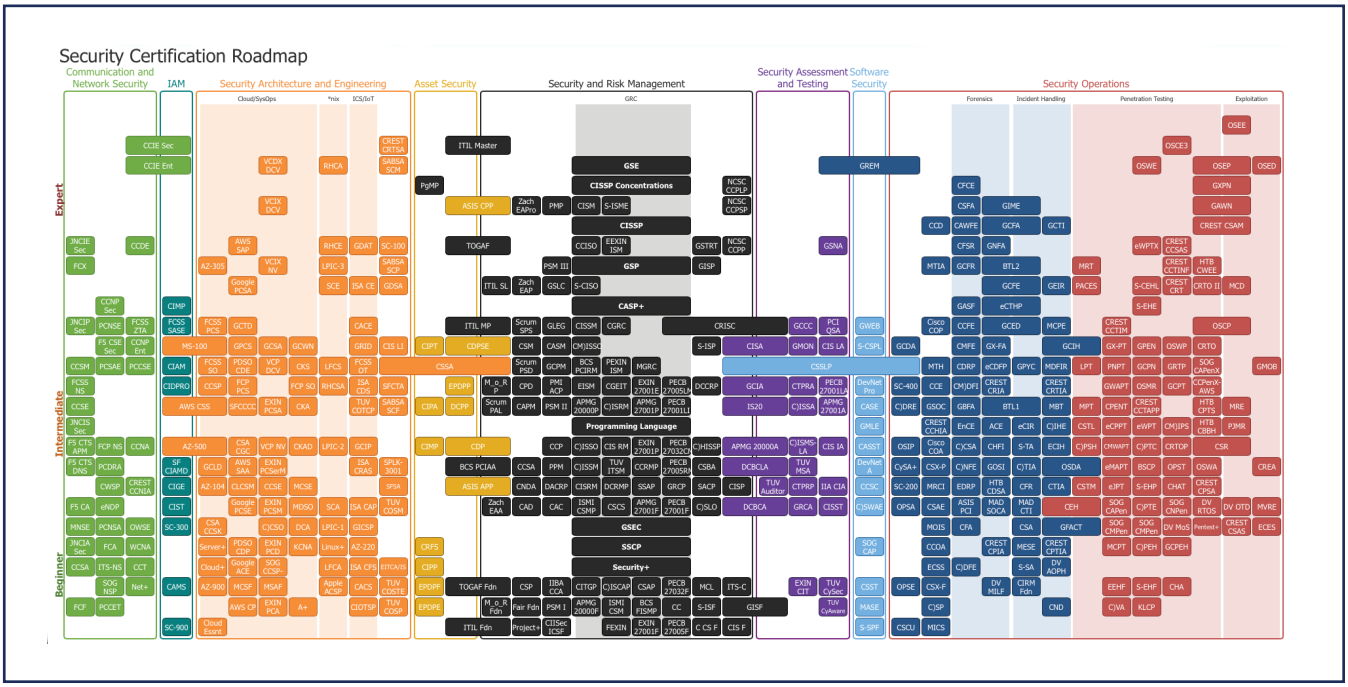


Figure 1: Security Certification Roadmap (Jerimy, 2024 at https://pauljerimy.com/security-certification-roadmap/)

CYBERSECURITY

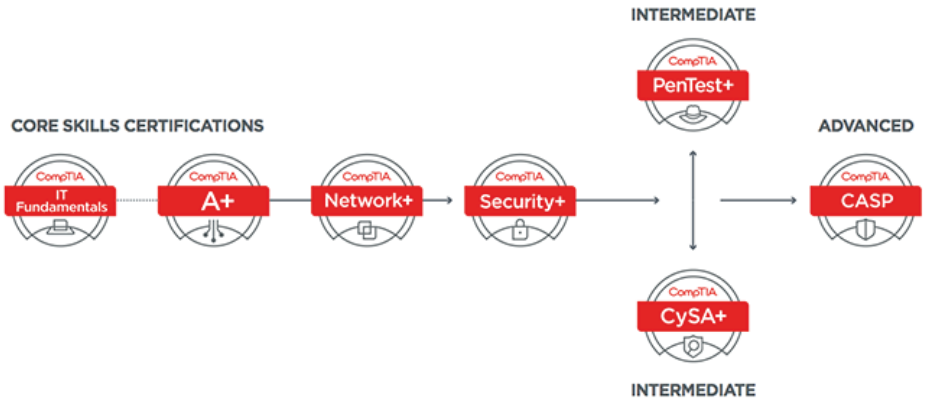
INDUSTRY CERTIFICATIONS

CompTIA – Computing Technology Industry Association

CompTIA certifications are some of the most highly recognized IT certifications available. CompTIA provides certifications across IT fields including software development, computer networking, cloud computing, and information security. CompTIA certifications are DoD 8140-approved baseline credentials for many work roles. The recommended cybersecurity pathway:

- **ITF+ (IT Fundamentals+):** Pre-career; basic IT literacy; suitable for high school and early college students exploring the field.
- **CompTIA A+:** Entry-level IT technician foundational credential; required baseline for many IT and security roles.
- **CompTIA Network+:** Networking fundamentals, protocols, and architecture; recommended before Security+.
- **CompTIA Security+ :** Ideal launchpad for a cybersecurity career; covers network security, threats, risk, and cryptography; widely required by employers and DoD 8140-approved for multiple work roles.
- **CompTIA CySA+ (Cybersecurity Analyst):** Intermediate; prepares for cybersecurity analyst roles; behavioral analytics and threat detection; DoD 8140-approved.
- **CompTIA PenTest+:** Intermediate; penetration testing and vulnerability assessment methodology.
- **CompTIA CASP+ (Advanced Security Practitioner:** Advanced; tailored for experienced practitioners, security architects, and senior engineers; DoD 8140 IAT Level III approved.

Security+ is the single most widely required entry-level security certification across both government and private sector employers. Most cybersecurity students should prioritize this first after completing foundational IT coursework.



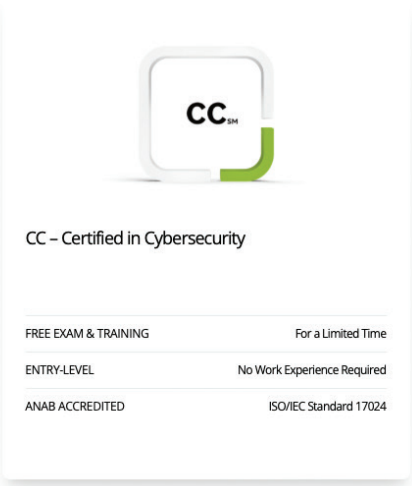
CYBERSECURITY

INDUSTRY CERTIFICATIONS

ISC2 - The International Information System Security Certification Consortium

ISC2 is the world's leading cybersecurity professional organization, a nonprofit with more than 600,000 certified members worldwide (ISC2, 2024). ISC2 certifications span from entry-level to senior executive credentials:

- **CC (Certified in Cybersecurity):** Entry-level; no experience required; ISC2 has offered free exam vouchers to students — verify current availability at isc2.org/Certifications/CC.
- **SSCP (Systems Security Certified Practitioner):** Associate-to-intermediate level; one year of experience; systems and network security focus.
- **CISSP (Certified Information Systems Security Professional):** Senior-level; five years of relevant experience; one of the most sought-after and esteemed certifications in the cybersecurity world; DoD 8140-approved; strongly recommended for anyone aspiring to security leadership.
- **CCSP (Certified Cloud Security Professional):** Cloud security architecture and governance; growing rapidly in demand.
- **CSSLP (Certified Secure Software Lifecycle Professional):** Secure software development and lifecycle management.



CYBERSECURITY

INDUSTRY CERTIFICATIONS

EC-Council

Rather than focusing on broad knowledge areas, EC-Council markets certifications toward specific roles and job titles. This makes it easy for those interested in a specific job to identify a relevant credential. Some EC-Council certifications may be too specialized for those seeking broad coverage. Key EC-Council certifications include:

- **CEH (Certified Ethical Hacker):** The most well-known EC-Council certification; widely recognized among security professionals and employers; while the title references "hacking," it is relevant for both offensive and defensive security professionals.
- **CND (Certified Network Defender):** Appropriate for those working in network administration or cybersecurity in roles such as network administrator, network engineer, or security analyst; applicable across cybersecurity operations roles.
- **CPENT (Certified Penetration Testing Professional):** Advanced penetration testing; for professionals with prior security experience seeking to specialize.
- **CHFI (Computer Hacking Forensic Investigator):** Digital forensics and incident response; chain of custody, evidence handling, and forensic investigation.

CORE	CORE	SPECIALIZE	EXECUTIVE
C|ND Certified Network Defender	C|EH Certified Ethical Hacker	C|HFI Computer Hacking Forensic INVESTIGATOR	C|CISO Certified Chief Information Security Officer
IAT Level I	CSSP Analyst	CSSP Infrastructure Support	IAM Level II
IAT Level II	CSSP Infrastructure Support	CSSP Incident Responder	IAM Level III
IAM Level I	CSSP Incident Responder		CSSP Manager
CSSP Infrastructure Support	CSSP Auditor		

CYBERSECURITY

INDUSTRY CERTIFICATIONS

GIAC - Global Information Assurance Certification (SANS Institute)

GIAC, founded in 1999 and affiliated with the SANS Institute, validates the skills of information security professionals. GIAC certifications are trusted by thousands of companies and government agencies, including the NSA. They are based on SANS training courses and are widely regarded as technically rigorous and role-specific. GIAC offers certifications in cyber defense, penetration testing, incident response, forensics, and more:

- **GSEC (GIAC Security Essentials):** Entry-level; validates hands-on knowledge of information security beyond terminology and concepts
- **GCFA (GIAC Certified Forensic Analyst):** Widely recognized forensic analyst certification covering advanced incident response, digital forensics, memory forensics, timeline analysis, anti-forensics detection, and threat hunting
- **GPEN (GIAC Penetration Tester):** Advanced penetration testing methodology and exploitation techniques
- **GCIH (GIAC Certified Incident Handler):** Incident response, intrusion analysis, and containment
- **GCIA (GIAC Certified Intrusion Analyst):** Network traffic analysis and intrusion detection

GIAC certifications are expensive but highly valued in technical and defense roles. Many employers, especially defense contractors, cover costs for mid-career professionals. SANS training is available through workforce development programs for students at reduced rates.

CYBERSECURITY

INDUSTRY CERTIFICATIONS

ISACA - Information Systems Audit and Control Association

ISACA was incorporated in 1969 by professionals who recognized a need for centralized guidance in auditing controls for computer systems. ISACA now serves over 165,000 members globally and offers certifications focused on governance, risk, audit, and management:

- **CISA (Certified Information Systems Auditor):** Widely recognized certification covering information security audit, control, assurance, and security governance; one of the most respected credentials for GRC and audit roles.
- **CISM (Certified Information Security Manager):** Designed for those demonstrating knowledge of information security management; a step above CISA in management focus.
- **CRISC (Certified in Risk and Information Systems Control):** Risk identification, assessment, evaluation, and management.
- **CSX-P (Cybersecurity Practitioner):** Entry-to-mid level technical practitioner credential.

Explore Have your students research three other certification bodies. What entry level and expert level (highest level) certifications do they provide?

CERTIFICATION BODY	ENTRY LEVEL	EXPERT LEVEL

VALUE OF

CERTIFICATIONS

Certifications are worth the time and effort you put into them.

Successfully completing a certification can lead to promotions, better job opportunities, or a salary increase. Surveys consistently show that earning a certification can result in a salary increase of up to 5% or more.

Distinction

Certifications set you apart from others competing for the same job. If two candidates are equally qualified but one holds a relevant certification, employers often choose the certified candidate. This is why it is recommended for college students to pursue certifications early — it helps differentiate them from other graduates who have similar coursework.

Accomplishment and Perseverance

Earning certifications demonstrates commitment and perseverance. It takes real effort, and having certifications shows dedication to your career and knowledge. They are especially important early in your career when you have limited job experience in the field.

Credibility

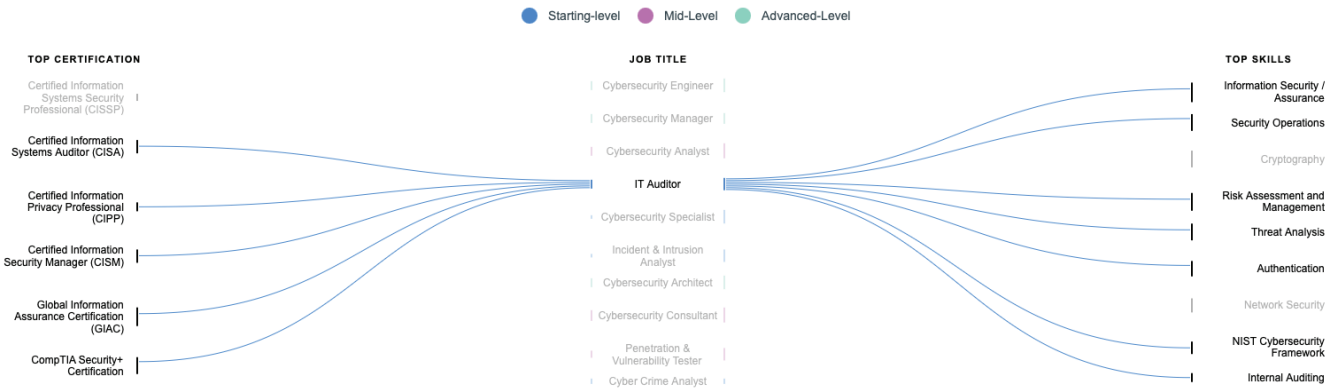
Certifications provide credibility. The professional community and employers view certifications as independent validation of your knowledge.

Unlike a training course, a certification signifies that your expertise has been verified by an external body. Certifications bring better job prospects, higher salaries, differentiation, recognition of commitment, and enhanced credibility.

CERTIFICATION

ROADMAP

The cybersecurity certification landscape is best understood as a pyramid, where basic certifications from each body serve as a foundation, and each mastery level (intermediate, advanced, expert) builds on that body of knowledge. Certifications are not only knowledge-level specific but also category specific — different certs address communication, assets, risk management, technical operations, and other domains. Building a thoughtful certification roadmap aligned to your target CWF 2.0 work role is essential for efficient career development.



Explore

Have your students explore the CyberSeek Interactive Tool.
https://www.cyberseek.org/certifications.html

What are the top three certifications? What are the jobs the certifications holders can aspire? What skills do students need to pass?

CERTIFICATION	JOB TITLE	TOP SKILLS

Note: For DoD and federal civilian positions, certifications are mandatory — not optional. DoD 8140 specifies required baseline certifications for each work role and proficiency level. Students targeting federal or defense careers should verify current requirements using the DoD Cyber Workforce Management System (CWMS).

PART VI

CYBERSECURITY SCHOLARSHIP PROGRAMS

CYBERSECURITY

SCHOLARSHIP PROGRAMS

Student Cybersecurity Scholarship Programs

The cybersecurity field has several scholarship programs specifically designed for students pursuing a career in the field. These programs can offer scholarships covering tuition, supplies, travel, and living allowances. Scholarships are offered based on a wide variety of criteria. Many are designed for specific populations including minority groups, women, veterans, and first-generation college students.

National Science Foundation CyberCorps® Scholarship Program

CyberCorps®: Scholarship for Service (SFS) is a unique program designed to recruit and train the next generation of cybersecurity professionals to meet the needs of Federal, State, local, and tribal governments. The program provides scholarships through qualified institutions of higher education to students enrolled in cybersecurity degree programs or cybersecurity-related fields. Scholarship recipients are required to work in a government cybersecurity position for a period equal to the length of their scholarship. Benefits include:

- Full tuition and mandatory fees
- Annual stipend of approximately $25,000 (undergraduate) to $34,000 (graduate)
- Professional development allowance for travel to job fairs
- Up to three years of support
- NSF maintains a job fair system connecting SFS graduates with government agencies

To date, over 5,000 students have received SFS scholarships and committed to government service across the country. The program is available at qualifying CAE-designated institutions.

More information: **sfs.opm.gov**

CYBERSECURITY

SCHOLARSHIP PROGRAMS

CIA Undergraduate Scholarship Program

For students interested in pursuing a government intelligence role after college, the CIA Undergraduate Scholarship Program may be a good fit. Requirements and benefits include:

- Must be enrolled full-time at an accredited college or university
- Must be a U.S. citizen with the ability to obtain and maintain a security clearance
- Tuition assistance up to $18,000 per calendar year for tuition, mandatory fees, and books
- Daily allowance for meals and incidentals during summer work tours at CIA headquarters
- Reimbursement for transportation costs between school and Washington, D.C.
- Upon graduation, recipients are required to work at the CIA for a period equal to 1.5 times the length of the scholarship received

More information: **cia.gov/careers/student-opportunities/**

Stokes Educational Scholarship Program (NSA)

The NSA Stokes Educational Scholarship Program is a scholarship for service administered by the National Security Agency (NSA). Like other scholarship-for-service programs, students who accept the Stokes scholarship agree to work with NSA after graduation or repay all scholarship funds received. Benefits include:

- Approximately $30,000 per year for tuition and fees
- Summer internships at NSA (approximately 3 months each summer) with paid compensation
- Offer of full-time employment at NSA upon program completion

Note: This scholarship is administered by the National Security Agency (NSA) — the U.S. intelligence and cybersecurity agency within the Department of Defense — NOT NASA (National Aeronautics and Space Administration).

Students should confirm program details and current award amounts at: intelligencecareers.gov/nsa

CYBERSECURITY

SCHOLARSHIP PROGRAMS

DoD SMART Scholarship for Service Program

The Science, Mathematics, and Research for Transformation (SMART) Scholarship, administered by the DoD, supports undergraduate and graduate students in STEM fields including cybersecurity. Benefits:

- Full tuition and education-related fees
- Annual stipend of $25,000–$38,000 depending on degree level
- Summer research internships at a DoD laboratory or facility
- Health insurance allowance
- Employment with a DoD facility upon graduation; service obligation of one year per year of support

SMART is ideal for students interested in DoD civilian careers and provides early exposure to DoD research environments. Applications open annually in the fall.

More information: **smartscholarship.org**

ISC2 Scholarships — Undergraduate and Graduate

The Center for Cyber Safety and Education and ISC2 offer both undergraduate and graduate scholarships ranging from $1,000 to $5,000 each. Key details:

- Any student studying in the cybersecurity field is eligible to apply regardless of citizenship
- Up to 20 scholarships awarded annually to undergraduate applicants
- Award funds are sent directly to the school to be applied to tuition, fees, and books
- ISC2 also offers free or discounted CC (Certified in Cybersecurity) certification opportunities for students — verify current availability at isc2.org

More information: **isc2.org/Certifications/CC** and the Center for Cyber Safety and Education: **iamcybersafe.org**

CYBERSECURITY

SCHOLARSHIP PROGRAMS

Cisco Snort Scholarship

The Snort scholarship is offered by technology firm Cisco in support of students pursuing cybersecurity. Those awarded the scholarship have received $10,000 to be used at an accredited college, university, or institution of their choice. Requirements include obtaining a high school diploma by the year the scholarship takes effect or demonstrating pursuit of a degree in an applicable field.

Note: Students should verify whether the Cisco Snort Scholarship is currently active and confirm current requirements and application windows directly with Cisco, as program terms may change from year to year.

Search "Cisco Snort Scholarship" on **cisco.com** for current information.

American Security Professional Fellowships (Heinz College, CMU)

Heinz College at Carnegie Mellon University awards a minimum scholarship of $10,000 per semester, up to a full tuition scholarship, to eligible students. Requirements include:

- U.S. citizenship
- Plans to enroll on a full-time basis in a qualifying Heinz College program
- Demonstrated strong commitment to the field of IT management, security, or public policy

More information: **heinz.cmu.edu**

GenCyber - NSA/NSF K-12 Cybersecurity Camps

The GenCyber program, funded by NSA and NSF, provides free cybersecurity summer camps for K-12 students and teachers. Camps are hosted by colleges and universities, often CAE-designated institutions. For high school students, GenCyber is often a first structured exposure to cybersecurity and can significantly increase post-secondary enrollment in cyber programs. Teachers may attend dedicated teacher-track GenCyber camps to build their own cybersecurity content knowledge.

More information: **gen-cyber.com**

CYBERSECURITY

SCHOLARSHIP PROGRAMS

AFCEA Educational Foundation Scholarships

The Armed Forces Communications and Electronics Association (AFCEA) Educational Foundation offers multiple scholarships specifically targeting cybersecurity, IT, and STEM students at the undergraduate and graduate levels. AFCEA scholarships are among the most well-funded and broadly available awards for students pursuing cyber-related degrees.

- **AFCEA Cyber Security Scholarship:** Awards up to $5,000 to U.S. citizens enrolled in a cyber-related degree program at a two- or four-year accredited institution. Preference given to students demonstrating financial need and a commitment to careers in government or defense.
- **AFCEA ROTC Scholarship:** Available to ROTC students in IT, cybersecurity, or related STEM fields. Awards vary by chapter and availability.
- **AFCEA Ralph W. Shrader Diversity Scholarship:** Supports underrepresented students — including women and minorities — pursuing graduate degrees in cyber, IT, or STEM disciplines. Award amounts up to $3,000.
- **AFCEA War Veterans Scholarship:** Supports U.S. military veterans enrolled in cyber or IT undergraduate programs. Particularly relevant for adult learners and career changers with military service.

How to Apply: Applications are submitted through the AFCEA Educational Foundation website. Deadlines vary by award; most open in the fall for spring awards. Advisors should encourage students to apply to multiple AFCEA scholarships simultaneously as eligibility criteria often overlap.

More information: **www.afcea.org/site/foundation** | Search: 'AFCEA scholarships cybersecurity'

Additional Scholarships to Explore

- Institution-specific cybersecurity scholarships at CAE-designated schools
- State workforce development grants — cybersecurity is on most state in-demand occupation lists
- WiCyS (Women in CyberSecurity) scholarships and conference fellowships: wicys.org
- National Cyber Scholarship Foundation (NCS) — merit-based for high school and college students
- ISACA scholarships for student members pursuing GRC certifications
- CompTIA and EC-Council training vouchers for students at qualifying institutions

PART VII

ESTABLISHING A CYBERSECURITY CAREER PATHWAY

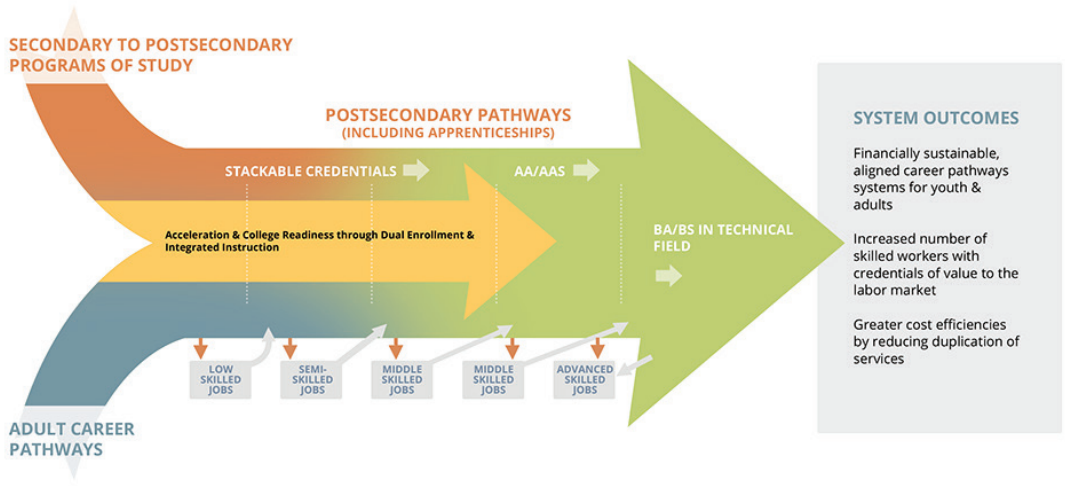
WHAT ARE

CAREER PATHWAYS

A Career Pathways System is about the coordination of people and resources to provide a more consistent system of education, training, and learning opportunities.

Career pathways can be defined as a sequence of career-focused classes, extracurricular experiences, industry credentials, and workforce readiness experiences like apprenticeships and internships that prepare students for future careers. In a career pathway, different programs and services are combined to help students develop important skills in academics, technical knowledge, and employability in the cybersecurity field.

A career pathways initiative involves partnerships between universities, four-year colleges, community colleges, primary and secondary schools, government agencies, employers, labor groups, and social service providers. These partnerships coordinate training options, academic credentials, industry certifications, and job placement. Well-designed career pathways eliminate duplication of courses, lower education costs, and give students an earlier start in reaching their career goals.



Career pathway models are used at the federal, state, and local levels. The Integrated Career Pathways model supports both high school age youth and adults, promoting collaboration, alignment, and cross-system development of structured pathways into and through postsecondary credential programs.

"Empowering Futures: Uniting Education and Industry in Cybersecurity Career Pathways"

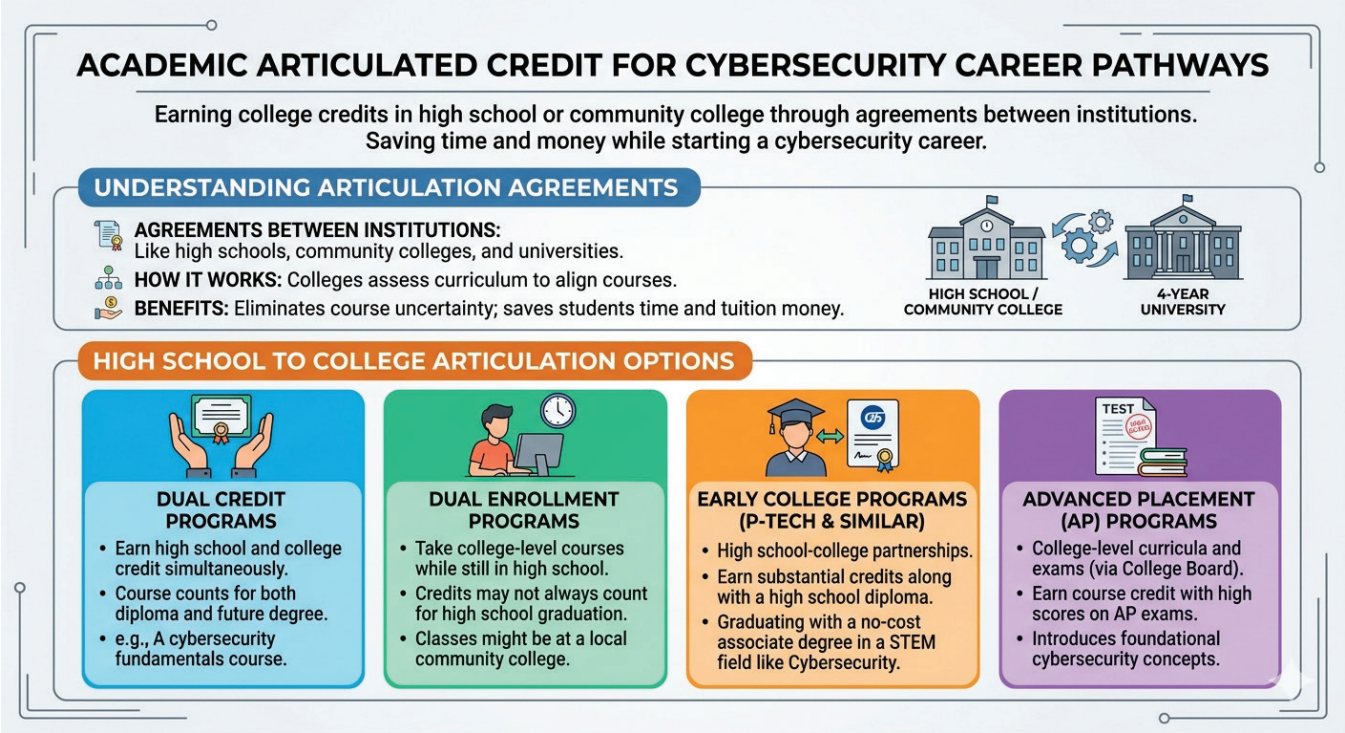
WHAT ARE

CAREER PATHWAYS

Academic Articulated Credit

One of the main goals of career pathways is to allow students to earn college credits while still in high school or while attending community college before transferring to a four-year institution. Articulation refers to the college credits that a student earns as part of an agreement between two or more educational institutions (high schools, community colleges, technical colleges, or universities) and their academic programs. These agreements are sometimes called transfer agreements, transfer guides, or transfer pathways.

Colleges and universities create articulation agreements after assessing curriculum, program learning outcomes, and instruction level. They agree on how courses completed at a community college will satisfy requirements at a four-year institution. This process involves academic departments working together to draft and publish guidelines — eliminating uncertainty about which courses to take and saving students time and money.



WHAT ARE

CAREER PATHWAYS

High School to College Articulation Options

Several options allow high school students to earn college credits before graduation. Exploring these options provides a head-start on higher education — especially in fast-paced fields like cybersecurity.

Dual Credit Programs

Dual Credit Programs allow high school students to earn both high school and college credit simultaneously. The coursework counts toward both a high school diploma and a future college degree. For example, a high school might offer a dual credit cybersecurity course covering fundamentals like data encryption and network security — content that aligns with a college-level course.

Dual Enrollment Programs - Like dual credit, dual enrollment allows students to take college-level courses while still in high school — but dual enrollment credits may not always count toward high school graduation requirements. Students may be required to take classes at a local community college while still attending high school. There may be application requirements, tuition requirements, and age restrictions.

Early College Programs (P-TECH and Similar)

Early college programs — like P-TECH (Pathways in Technology Early College High School) — are partnerships between high schools and colleges. These programs enable students to earn substantial college credits alongside their high school diploma, typically starting in their junior year. P-TECH allows students to graduate with both a high school diploma and a no-cost associate degree in a STEM field such as cybersecurity. These programs are designed for committed students seeking an early start in a specific career area.

Advanced Placement (AP) Programs

Advanced Placement (AP), run by the College Board, offers college-level curricula and examinations to high school students. Colleges and universities often grant course credit to students who earn high scores on AP examinations. Taking AP Computer Science Principles, for example, introduces key concepts foundational to cybersecurity. AP credits can reduce both time and tuition cost in college.

WHAT ARE

CAREER PATHWAYS

Summary Comparison of High School Credit Options:

Program	Description	HS Credit	College Credit	Real-world Experience
Dual Credit	Simultaneously earn high school and college credit by taking certain courses.	Yes	Yes	Depends on the course
Dual Enrollment	Enroll in college-level courses while in high school. These credits might not count toward high school requirements.	Varies	Yes	Depends on the course
Early College/P-TECH	Partnerships between high schools and colleges that enable students to earn substantial college credits alongside their high school diploma.	Yes (often enough for associate degree)	Yes	Depends on the program
Advanced Placement (AP)	College Board program offering college-level curricula and examinations to high school students. High examination scores can lead to college credit.	Yes (from the course)	Yes (from the exam)	No, typically classroom-based

WHAT ARE

CAREER PATHWAYS

Career and Technical Education (CTE) Pathways in Cybersecurity

Career and Technical Education (CTE) programs provide structured K-12 and community college cybersecurity pathways funded in part by the Strengthening Career and Technical Education for the 21st Century Act (Perkins V, 2018). CTE cybersecurity pathways are among the fastest-growing program areas nationally and represent an important bridge between secondary education and postsecondary credentials or careers.

What CTE Pathways Offer

- **Structured course sequences:** Students complete a multi-year sequence (typically three courses) that progresses from foundational to advanced cybersecurity concepts, aligned with standards like NICE CWF 2.0 and CompTIA certifications.
- **Industry-recognized credentials (IRCs):** Many CTE programs prepare students for certifications such as CompTIA ITF+, A+, Security+, or EC-Council CEH—credentials valued in college admissions and hiring.
- **Dual enrollment and articulation agreements:** Students may earn college credit through partnerships with local colleges and universities, reducing time and cost to complete a degree.
- **Work-based learning:** Perkins V emphasizes real-world experience, with programs offering job shadowing, internships, apprenticeships, or employer partnerships in cybersecurity.

Finding CTE Programs

- **State CTE offices:** Each state's Department of Education publishes approved CTE program frameworks and course catalogs. Search '[state] CTE cybersecurity pathway' to locate local offerings.
- **CYBER.ORG:** A national K-12 cybersecurity education nonprofit that provides curriculum, teacher training, and program support for CTE pathways. Visit cyber.org for curriculum maps and state-level program directories.
- **National Centers of Academic Excellence (NCAE-C):** NSA-designated K-12 NCAE-C schools offer rigorous cybersecurity programs. Use the NCAE-C program map at nsa.gov to find designated schools near you.
- **Perkins Collaborative Resource Network (PCRN):** The U.S. Department of Education's clearinghouse for CTE resources: cte.ed.gov.

Advisor Tip

When meeting with high school students who are already in a CTE cybersecurity pathway, ask about dual enrollment and articulation agreements. Students who have completed CTE sequences may arrive at college with 6-18 credits already earned — a significant advantage in time-to-degree.

CENTERS OF

ACADEMIC EXCELLENCE

Centers of Academic Excellence in Cybersecurity (NCAE-C/CAE)

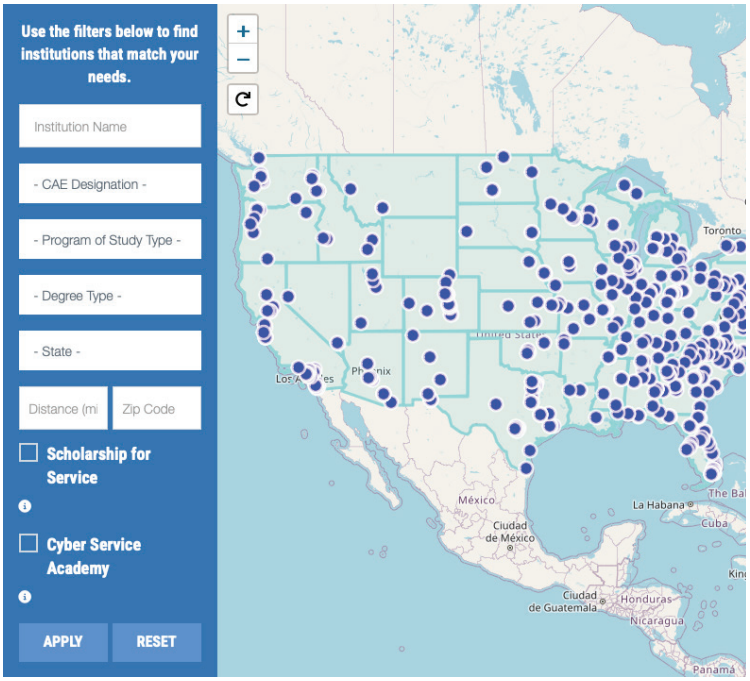
The National Security Agency (NSA) created the Centers of Academic Excellence in Cybersecurity (CAE) program to help colleges and universities prepare students for real-world cybersecurity careers. If you choose a CAE-designated school, it means the program meets high national standards and aligns with the NICE Cybersecurity Workforce Framework—a model used by employers to define cybersecurity roles and the skills needed for them. In short, you can feel confident that what you're learning is relevant, practical, and recognized by employers and federal agencies.

There are three main types of CAE-designated institutions, each offering a slightly different focus:

- **CAE-CD (Cyber Defense):** These programs concentrate on protecting systems and data and are the most common and widely available at both community colleges and universities. They prepare students for roles such as security analyst, network defender, and risk or compliance specialist. An example of a CAE-CD institution is the University of Maryland.

- **CAE-R (Cybersecurity Research):** These institutions focus on advancing the field through research and innovation. They are typically research universities and are a strong fit for students interested in graduate school or contributing to new cybersecurity technologies. An example is the Massachusetts Institute of Technology.

- **CAE-CO (Cyber Operations):** These programs offer highly technical, interdisciplinary training that includes offensive security, cyber operations, and intelligence work. They tend to be more specialized and selective. An example is the United States Air Force Academy.



Choosing a CAE-designated institution can give you a competitive advantage as you enter the cybersecurity field. It signals to employers that you've received a high-quality education and may provide access to valuable opportunities such as federal internships and scholarships, including programs like CyberCorps SFS.

To explore CAE-designated schools by location, you can visit [maps.caecommunity.org.](maps.caecommunity.org)

WHAT ARE

PROGRAMS OF STUDY

Programs of Study (POS): A program of study is the complete set of courses you'll take to earn a specific degree.

This includes your major requirements, any concentration or minor, and the overall catalog requirements set by the college. As you explore programs, it's important to look beyond the degree title and examine what you'll actually learn. Strong cybersecurity programs clearly outline how their courses connect to real-world careers.

One key indicator is whether the curriculum is aligned to the NICE Cybersecurity Workforce Framework, which defines the knowledge, skills, and tasks (often called T-K-S statements) needed for specific cybersecurity roles. Programs mapped to this framework—especially those at CAE-designated institutions—are intentionally designed to prepare you for jobs you can step into after graduation, not just theoretical knowledge.

Why This Matters

Choosing a program with a well-structured POS helps ensure you're building relevant, job-ready skills throughout your coursework. It also makes it easier to understand how classes connect to careers like security analyst, digital forensics examiner, or cybersecurity policy specialist.

Beyond individual programs, CAE-designated schools are part of a national network led by the National Security Agency. These institutions collaborate with one another, share best practices, and continuously improve cybersecurity education. As a student, this means you may benefit from stronger curricula, access to shared resources, research opportunities, and connections to a broader cybersecurity community—all of which support your transition into the workforce and contribute to protecting the nation's digital infrastructure.

UNDERSTANDING

SECURITY CLEARANCES

Many of the most sought-after and highest-compensated cybersecurity positions — in federal agencies, the Department of Defense, intelligence community, and government contracting firms — require employees to hold a U.S. government security clearance.

For students pursuing these career paths, understanding what clearances are, how they are obtained, and how to maintain eligibility is an essential part of career planning that should begin well before graduation.

What Is a Security Clearance?

A security clearance is an official determination by the U.S. government that an individual is trustworthy, reliable, and loyal enough to access classified national security information. Clearances are not applied for by individuals directly — they are sponsored by an employer (a federal agency or cleared government contractor) who has identified a position that requires access to classified information. Students cannot obtain a clearance on their own; the process begins when they accept a position that requires one.

Clearance Levels

The U.S. government issues several tiers of clearance, each granting access to progressively more sensitive classified information. Advisors should help students understand which level their target role is likely to require:

- **Public Trust (IT-I, IT-II, IT-III):** Not technically a clearance, but a background investigation required for federal IT and cybersecurity positions that handle sensitive but unclassified data. Often required for entry-level federal IT roles and contractor positions. The most accessible starting point for students entering federal service.
- **Confidential:** Grants access to information whose unauthorized disclosure could damage national security. Relatively common for administrative and support roles. Required investigation is less intensive than Secret.
- **Secret:** The most commonly held clearance level for cybersecurity professionals in defense and federal IT roles. Grants access to information whose unauthorized disclosure could cause serious damage to national security. Investigation covers the past 7 years of background, finances, foreign contacts, and character. Typical adjudication timeline: 3–6 months, though timelines vary.
- **Top Secret (TS):** Required for roles involving highly sensitive national security information. Investigation is substantially more intensive than Secret, covering the past 10 years of background. Typical adjudication timeline: 6–12 months or longer.
- **Top Secret / Sensitive Compartmented Information (TS/SCI):** The highest standard clearance, required for roles in the intelligence community (NSA, CIA, DIA, NRO, and others) and advanced cyber operations. In addition to a full-scope background investigation, TS/SCI positions often require a polygraph examination. Students pursing NSA Stokes, CIA, or similar scholarship-for-service programs will typically require this level.

UNDERSTANDING

SECURITY CLEARANCES

How the Clearance Process Works

Once an employer sponsors a candidate, the process follows these general steps:

1. **SF-86 (Questionnaire for National Security Positions):** The applicant completes a detailed federal form covering personal history, employment, education, finances, foreign contacts, mental health treatment, drug use, and criminal history. Accuracy and completeness are critical — deliberate omissions or false statements are grounds for denial and may constitute a federal offense.
2. **Background Investigation:** Conducted by the Defense Counterintelligence and Security Agency (DCSA) or the relevant agency. Investigators interview references, neighbors, former employers, and colleagues. Financial records, court records, and foreign travel history are reviewed.
3. **Adjudication:** A trained adjudicator reviews the investigation results against the 13 Adjudicative Guidelines (which cover areas such as financial considerations, foreign influence, personal conduct, drug involvement, and allegiance to the U.S.) and makes a suitability determination. The process is holistic — issues in one area can be mitigated by positive factors in others.
4. **Polygraph (for some positions):** TS/SCI and many intelligence community positions require a counterintelligence (CI) polygraph or full-scope polygraph. Students should be aware of this requirement when targeting intelligence community roles.

What Can Affect Clearance Eligibility?

The adjudication process is holistic and considers the totality of an individual's background. Conditions that may raise concerns — but are not automatic disqualifiers — include:

- **Financial Issues:** Debt, delinquent accounts, bankruptcy, or poor financial habits are common causes of delays or denials. Students should build strong financial habits early and resolve issues before the clearance process.
- **Foreign Contacts and Travel:** Ties to foreign nationals, dual citizenship, or extensive travel may raise concerns. These do not disqualify applicants but must be fully and honestly disclosed.
- **Drug Use:** Recent or frequent illegal drug use is a concern, especially for TS/SCI roles. Marijuana use—even where legal—can impact federal suitability decisions.
- **Criminal History:** Arrests and convictions are reviewed in context. Minor or juvenile offenses are not automatic disqualifiers, but felonies and repeated offenses raise concern. Honesty is critical.
- **Online Activity and Social Media:** Public posts and digital activity are reviewed. Content suggesting extremism, disloyalty, or dishonesty—even from years ago—can affect adjudication.

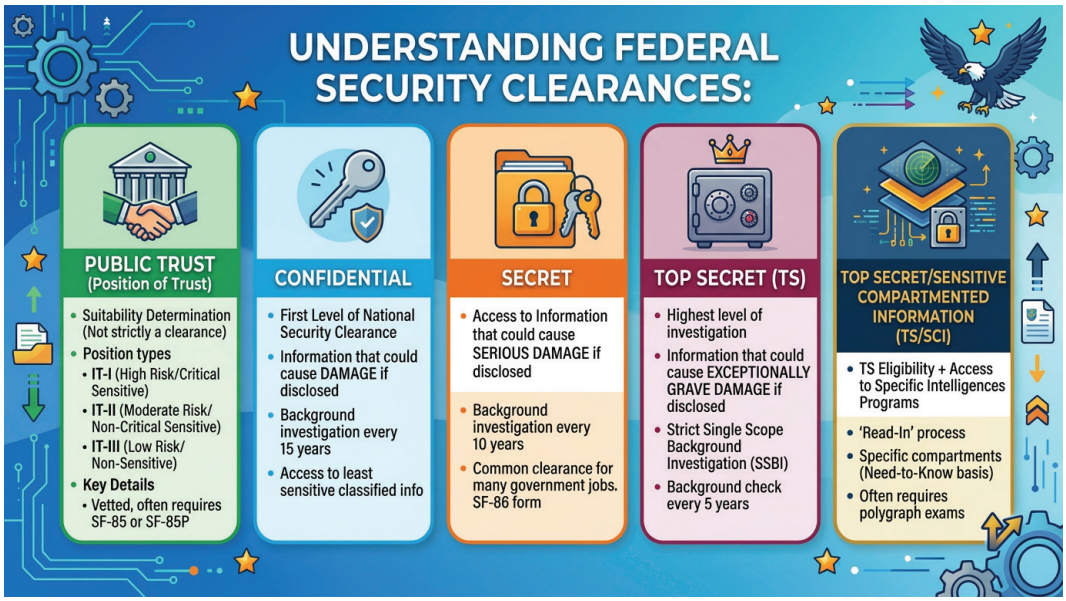
UNDERSTANDING

SECURITY CLEARANCES

Clearances and CWF 2.0 / DCWF

Under the DoD Cyberspace Workforce Framework (DCWF) and DoDM 8140.03, virtually all designated DoD cyber positions require at minimum a Secret clearance as a condition of employment. Many advanced work roles in the Protect and Defend, Analyze, and Cyberspace Effects categories require TS or TS/SCI. Students who complete CyberCorps SFS, NSA Stokes, or DoD SMART scholarship programs will enter federal service with their clearance sponsored as part of their service obligation — a significant career advantage.

Students can search cleared cybersecurity positions on USAJobs (usajobs.gov) and ClearanceJobs (clearancejobs.com). Clearance level required is listed on each position.



Advisor Tip

When advising students interested in federal or defense cybersecurity careers, ask early: 'Are you a U.S. citizen?' Non-U.S. citizens are generally not eligible for security clearances, which closes most federal and DoD cybersecurity pathways. This is important to address honestly and early so students can focus on the pathways available to them. Also remind students: start building a clean, responsible record NOW — the clearance process reviews years of history, not just who you are today.

MAINTAINING A POSITIVE

DIGITAL FOOTPRINT

In cybersecurity, what you do online matters twice!

Once as a future professional in a field that demands integrity and trustworthiness, and once as a candidate whose online history will be reviewed by potential employers and — for government roles — federal background investigators. A positive digital footprint is no longer optional for students pursuing cybersecurity careers. It is part of career readiness, and the time to build it is now.

What Is a Digital Footprint?

Your digital footprint is the complete record of your online activity — everything that can be found about you by searching the internet. It includes two components, Active and Passive.

For cybersecurity candidates, both components are relevant. Employers conduct informal online searches as a standard part of hiring. Federal background investigators formally review publicly accessible online activity as part of the SF-86 adjudication process.

Why It Matters for Cybersecurity Careers

- **Clearance Eligibility:** The 13 Adjudicative Guidelines explicitly include 'personal conduct' as a factor. Online statements suggesting dishonesty, extremist views, foreign loyalties, or illegal activity — even from years earlier — can delay or jeopardize a clearance determination. Investigators search publicly accessible social media by name and known usernames.
- **Employer Screening:** A 2023 CareerBuilder survey found that over 70% of employers search candidates online before interviews, and nearly half found content that caused them to reject a candidate. Cybersecurity employers — who are specifically in the business of assessing risk and trust — apply this scrutiny more rigorously than most.
- **Professional Reputation:** The cybersecurity community is relatively small and interconnected. Posts, forum comments, and online interactions that demonstrate expertise, professionalism, and integrity build reputation over time. The inverse is equally true.
- **GitHub and Portfolio Visibility:** For technical roles, your GitHub profile, open-source contributions, and project portfolio are a positive form of digital footprint that directly demonstrates skill. Employers and recruiters actively search these. A well-maintained GitHub is a career asset.

MAINTAINING A POSITIVE

DIGITAL FOOTPRINT

What Students Should and Shouldn't Do

Starting Now: A First-Week Digital Footprint Checklist

1. **This Week:** Google your name. Review all public social media accounts. Create or update your LinkedIn profile. Create a GitHub account if you do not have one.
2. **This Semester:** Post your first GitHub repository (a class project, lab writeup, or simple tool). Connect with your instructors and at least 10 cybersecurity professionals on LinkedIn. Join one student chapter (ISACA, ISC2, or WiCyS).
3. **Before Graduation:** Have a complete LinkedIn profile with recommendations. Maintain a GitHub with at least 5 substantive projects. Have participated in at least one public-facing cyber community (competition, blog, open-source contribution). Run a final self-audit of your digital footprint before beginning your job search.

Explore

Search your own name in Google right now. What appears in the first three pages of results? Is any of it something you would want a federal investigator or a hiring manager to see? What is missing that you wish were there? Use this as the starting point for your digital footprint plan.

Advisor Tip

Frame the digital footprint conversation with students as a long-term investment, not just risk avoidance. A well-built professional online presence — LinkedIn, GitHub, competition records, community participation — is one of the highest-return career investments a student can make while still in school. Many cybersecurity employers report that a strong GitHub portfolio carries more weight than GPA in technical hiring decisions.

Creating Your Unique

CAREER PATHWAYS

Are you ready to forge your unique path towards a rewarding career in cybersecurity? Let's explore the importance and the steps involved in creating a personal career pathway plan, a professional blueprint that aligns with your personal goals and aspirations.

Why is a Career Pathway Plan Important?

A career pathway plan can act as your roadmap, guiding you towards your dream job in cybersecurity. It helps you assess your strengths, work on your weaknesses, and align your interests with potential career options.

Creating Your Career Pathway Plan: A Step-by-Step Guide

1. **Self Evaluate:** Begin by assessing your strengths and weaknesses. Are you good at problem-solving or coding but struggle with time management? Also identify your interests. Do you enjoy learning about network security or are you more drawn to governance, policy, or investigation? Use the NICE CWF 2.0 interactive tool to browse work roles and identify which ones resonate with your interests.

2. **Explore Career Options:** Research different careers within the cybersecurity field. Look at job descriptions, requirements, and necessary skills on job boards (USAJobs, LinkedIn, Indeed, ClearanceJobs for cleared roles). Use CyberSeek to understand local job demand. Explore CYBER.ORG career profiles and trycyber.us.

3. **Plan your Path:** Utilize resources available at school or online to develop your plan. This might involve meeting with teachers, career counselors, and academic advisors. Ask about opportunities to earn college credit while still in high school — dual credit, dual enrollment, early college, or AP programs. Identify CAE-designated institutions that offer programs aligned to your target career.

4. **Engage Your Support Network:** Involve teachers, counselors, parents, and community mentors in your planning process. They can provide valuable advice and feedback on your career pathway plan. Seek assistance selecting classes, preparing for industry certifications, and completing college applications. Look for student organizations, conferences, job fairs, and internship or apprenticeship programs.

5. **Set Personal Goals:** Define specific, measurable, achievable, relevant, and time-bound (SMART) goals. For example: "I will earn CompTIA Security+ by the end of my junior year" or "I will attend a GenCyber camp this summer" or "I will complete my application to a CAE-designated institution by November."

6. **Monitor Your Progress:** Regularly revisit your plan and track your progress towards your goals. Adjust your plan as needed based on your accomplishments, industry and technology trends and evolving interests.

Creating Your Unique

CAREER PATHWAYS

Further Tips for Your Career Pathway Journey

- **Stay Current with Trends:** Keep abreast of the latest developments in cybersecurity. Follow news sources like Krebs on Security, Dark Reading, and CISA alerts. This knowledge can inform your plan and help you make strategic decisions about specialization.

- **Embrace Technology:** The cybersecurity sector is deeply intertwined with technological advancement. Stay current on technologies such as artificial intelligence (AI), machine learning in security, cloud computing, secure communications, virtualization, and smart/IoT devices — all of which are reshaping how security professionals do their jobs.

- **Fuel Your Passion:** Embrace opportunities that a cybersecurity career pathway offers: competitions, internships, research projects, and exchange programs. Your enthusiasm can inspire others to support your plan and opens doors to mentors and sponsors in the field.

- **Network:** Build relationships with teachers, advisors, fellow students, and professionals in the field. Attend local ISACA, ISSA, and ISC2 chapter events. Join LinkedIn and connect with cybersecurity professionals. Networking is a two-way street; strive to assist others in their professional journeys too.

Remember: creating a personalized career pathway plan is your first step toward a fulfilling career in cybersecurity. Use this guide as a starting point and shape your unique path to success.

PART VIII

EXTRACURRICULAR ACTVITIES

EXTRACURRICULAR

ACTIVITIES

Extracurricular activities provide a channel for reinforcing lessons learned in the classroom, offering students the opportunity to apply academic skills in real-world contexts.

This is particularly important for cybersecurity students — it enables them to build skills in critical thinking, problem-solving, and teamwork.

A Cybersecurity Club is a student-run organization providing outside-of-class activities relevant to the cybersecurity industry. Participants leave with valuable experience proven useful during interviews and on the job.

Student cybersecurity competitions provide a fun and interesting way to exercise technical skills, identify and recognize cybersecurity talent, and engage students with real professional challenges. They let students experience how organizations must deal with the constant threat of cyber-attacks. Each competition below includes its updated NICE CWF 2.0 alignment.

Popular Student Cybersecurity Competitions

1. **CyberPatriot** is a program established for the K-12 education of students in cybersecurity by the Air Force Association. There are three branches of the program, including the National Youth Cyber Defense Competition, AFA CyberCamps, and Elementary School Cyber Education Initiative. The Cyber Defense Competition starts at the state and then regional level. Top competitors are then given an all-expense paid trip to the national finals. At nationals, participants compete for national recognition and scholarship money.

    - ***CWF 2.0 Alignment:*** Protect and Defend (PD) & Operate and Maintain (OM)
    - ***Key Skills Developed:*** System hardening, firewall configuration, user account management, network defense, security auditing
    - ***Website:*** https://www.uscyberpatriot.org

2. **CSAW Capture the Flag (CTF)** is the most comprehensive student-run cybersecurity event in the world, featuring nine hacking competitions, workshops, and industry events. Final events are hosted by six global academic centers. CSAW draws thousands of student competitors annually and is used by employers to identify top talent.

    - ***CWF 2.0 Alignment:*** Protect and Defend (PD), Analyze (AN), & Operate and Maintain (OM)
    - ***Key Skills Developed:*** Skills vary by individual challenge; typically includes web exploitation, reverse engineering, cryptography, forensics, and binary exploitation
    - ***Website:*** https://www.csaw.io

EXTRACURRICULAR

ACTIVITIES

Popular Student Cybersecurity Competitions (cont.)

3. **The National Cyber League (NCL)**, powered by Cyber Skyline, enables students to prepare and test themselves against practical cybersecurity challenges they will likely face in the workforce — such as identifying hackers from forensic data, pentesting and auditing vulnerable websites, recovering from ransomware attacks, and more. Open to U.S. high school and college students, NCL provides a Scouting Report for each participant detailing performance by skill category — a powerful portfolio tool for job applications.

    - ***CWF 2.0 Alignment:*** Protect and Defend (PD), Analyze (AN), & Operate and Maintain (OM)
    - ***Key Skills Developed:*** Open-source intelligence (OSINT), cryptography, log analysis, network traffic analysis, password analysis, web application security, digital forensics
    - ***Website:*** https://nationalcyberleague.org

4. **MITRE Cyber Academy** presents an annual STEM Capture the Flag challenge open to both current students and professionals. While professionals may compete for educational purposes, only eligible high school and college teams can win prizes, scholarships, and internship opportunities. MITRE is a federally funded research and development organization with deep ties to national security and cybersecurity.

    - ***CWF 2.0 Alignment:*** Protect and Defend (PD) & Analyze (AN)
    - ***Key Skills Developed:*** Steganography, software exploitation, computer forensics, cryptography, networking, reverse engineering
    - ***Website:*** https://mitrecyberacademy.org

5. **The NSA Codebreaker Challenge** provides students with a hands-on opportunity to develop reverse-engineering and low-level code analysis skills while working on a realistic problem set centered around the NSA's mission. The challenge is released annually and students work independently or in teams over several months. It is one of the most technically demanding student challenges available and is highly regarded by intelligence community and defense employers.

    - ***CWF 2.0 Alignment:*** Securely Provision (SP)
    - ***Key Skills Developed:*** Reverse engineering, encryption algorithms, steganography, digital forensics, cryptography, networking, low-level code analysis
    - ***Website:*** https://codebreaker.ltsnet.net/challenge

EXTRACURRICULAR

ACTIVITIES

Popular Student Cybersecurity Competitions (cont.)

6. **PicoCTF** is a free computer security game targeted at middle and high school students, created by security experts at Carnegie Mellon University. The game consists of a series of challenges centered around a unique storyline where participants must reverse-engineer, break, hack, decrypt, or do whatever it takes to solve each challenge. picoCTF is one of the best entry-level competitions for students with no prior CTF experience and is an excellent first step before more advanced competitions like NCL or CSAW.

    - *CWF 2.0 Alignment:* Protect and Defend (PD), Analyze (AN), & Operate and Maintain (OM)
    - *Key Skills Developed:* Web exploitation, cryptography, binary exploitation, forensics, reverse engineering — structured for beginners
    - *Website:* https://picoctf.com

7. **The Collegiate Cyber Defense Competition (CCDC)** is the nation's largest and most employer-recognized collegiate defensive cyber competition. Unlike offense-focused CTF competitions, CCDC tests students' ability to defend live network environments against a professional red team — simulating the real-world responsibilities of a defensive security operations center (SOC) team under pressure.

    - *CWF 2.0 Alignment:* Protect and Defend (PD), Operate and Maintain (OM), & Oversee and Govern (OV)
    - *Key Skills Developed:* Network defense and intrusion detection (Snort, Suricata, Zeek), Operating system hardening (Windows Server, Linux), Firewall and access control configuration, Incident response and forensic documentation, Log analysis and SIEM use (Splunk, ELK), Business communication and time-pressured decision making
    - *Website:* nationalccdc.org | To find your regional competition: Search "CCDC [your region] collegiate cyber defense"

Advisor Tip

CCDC is widely regarded as the most direct college-to-employer pipeline competition in defensive security. Encourage students interested in SOC analyst, network defender, or incident response careers to join or start a CCDC team. Many coaches report that top performers receive job offers before graduation.

BUILDING A

SECURITY PORTFOLIO

Employers increasingly expect candidates to demonstrate skills beyond the degree and certification.

Document and present your achievements proactively:

- CTF challenge writeups published on a personal blog or GitHub
- NCL Scouting Report (download and save after each season)
- CCDC and CyberPatriot participation records and roles played
- Home lab documentation (network diagrams, configurations, experiment logs)
- Security research projects, academic papers, or capstone projects
- Open-source tool contributions or responsible vulnerability disclosures

A well-curated GitHub profile, a LinkedIn page with NICE CWF 2.0 role alignment, and a brief portfolio site can significantly differentiate a candidate in a competitive job market.

Professional Organizations and Student Chapters

Engaging in professional organizations and student chapters helps you build a strong network, gain industry insight, and access valuable resources beyond the classroom. These groups provide opportunities for mentorship, leadership development, scholarships, and exposure to real-world cybersecurity practices—helping you stay current and competitive as you enter the field.

1. **ISACA Student Chapters:** GRC, audit, and governance focus; access to ISACA resources, networking events, and member scholarships.
2. **ISC2 Student Chapters:** Broad cybersecurity networking; CC certification outreach; access to ISC2 career resources and events.
3. **WiCyS (Women in CyberSecurity):** Scholarships, mentoring, conferences, and a strong community for women in the field: wicys.org.
4. **ISSA (Information Systems Security Association):** Local chapter events, networking with regional employers, discounted student membership.
5. **IEEE Computer Society:** Technical and research-oriented; relevant for students in CS and engineering disciplines.
6. **SANS/GIAC Community:** Access to SANS webcasts, community resources, and student pricing on selected courses.

QUICK REFERENCE

KEY RESOURCES AND URLs

Resource	URL	Purpose
NICE CWF 2.0 Interactive Tool	niccs.cisa.gov/workforce-framework	Browse all 41 work roles; TKS statements
NIST SP 800-181r2	doi.org/10.6028/NIST.SP.800-181r2	Full CWF 2.0 specification
DCWF / DoD 8140	dodcio.defense.gov/Cyber-Workforce/DCWF/	DoD cyberspace workforce roles and qualifications
NCWES 2023	whitehouse.gov (search "NCWES 2023")	National Cyber Workforce & Education Strategy
CyberSeek Pathway	cyberseek.org/pathway.html	Entry/mid/advanced job pathway tool
CyberSeek Heat Map	cyberseek.org/heatmap.html	Real-time state/metro job demand
CyberSeek Certifications	cyberseek.org/certifications.html	In-demand certs and associated job roles
CAE Institution Finder	caecommunity.org/find-a-cae	Find NCAE-C schools by state and designation
CyberCorps SFS	sfs.opm.gov	Scholarship for Service program
DoD SMART Scholarship	smartscholarship.org	DoD SMART scholarship information
NSA Stokes Scholarship	intelligencecareers.gov/nsa	NSA educational scholarship program
CIA Undergraduate Scholarship	cia.gov/careers/student-opportunities/	CIA undergraduate scholarship program
GenCyber	gen-cyber.com	K-12 cybersecurity camp finder
CYBER.ORG Career Profiles	cyber.org/career-exploration/cyber-career-profiles	K-12 career awareness profiles
trycyber.us	trycyber.us	14 virtualized cybersecurity career challenges
CyberPatriot	uscyberpatriot.org	K-12 national cyber defense competition
CSAW CTF	csaw.io	Premier student-run global CTF
National Cyber League	nationalcyberleague.org	Collegiate CTF with skills scouting report
MITRE Cyber Academy	mitrecyberacademy.org	Federal STEM CTF with scholarships
NSA Codebreaker Challenge	https://nsa-codebreaker.org/home	Advanced annual reverse-engineering challenge
picoCTF	picoctf.com	Beginner-friendly K-12/college CTF

QUICK REFERENCE

KEY RESOURCES AND URLs

Resource	URL	Purpose
CTFtime.org	ctftime.org	Global CTF competition calendar
TryHackMe	tryhackme.com	Beginner-friendly guided security learning
CCDC	https://www.nationalccdc.org/	Advanced competition where team defends live network
Hack The Box	hackthebox.com	Intermediate/advanced hands-on platform
USAJobs Cyber	usajobs.gov/cybersecurity	Federal cyber jobs and Pathways internship
WiCyS	wicys.org	Women in CyberSecurity — events and scholarships
ISC2 CC Certification	isc2.org/Certifications/CC	Free or low-cost entry-level ISC2 cert for students

This toolkit was updated in 2025 to reflect NICE CWF 2.0 (NIST SP 800-181r2), DCWF/DoD 8140.03, NCWES 2023, and current workforce statistics. All URLs and program details should be verified for currency. This toolkit is intended as an advising resource and does not constitute official career, legal, or financial aid counsel. EPNC Career Counselors and Academic Advisors.

exploreCyber

Visit us at:

ExplorCyber.org

ExploreCyber, a Cybersecurity Career Awareness and Exploration Initiative (CCAEI), is funded by
the National Science Foundation (NSF) Advanced Technological Education (ATE) Program, Grant #2500740.