FedVTE FEDERAL VIRTUAL TRAINING ENVIRONMENT

Cybersecurity Training and Education for Veterans

A User Guide for U.S. Veterans Entering the Cybersecurity Career Field.

Homeland Security

FedVTE FEDERAL VIRTUAL TRAINING ENVIRONMENT

Inside this guide

Homeland Security

Getting Started

Transitioning from a military career to civilian life just got easier. This guide introduces Veterans to cybersecurity training and education resources that help build the skills necessary to transition into a cybersecurity career.

What is Cybersecurity?

Cybersecurity focuses on protecting computers, networks, and information from unauthorized access or attack. Essentially, **if a device connects to the Internet**, it is vulnerable to attacks and needs protecting.

Through military service, Veterans may come equipped with the ability to quickly process information for security decisions, maintain situational awareness, learn on the job, and respond to challenging situations; these abilities can transfer successfully into a cybersecurity career.

Cybersecurity is a field that allows Veterans to transfer a passion for defending our country to a new battlefield – one that has an ever-changing landscape with many adversaries. Cybersecurity careers are an opportunity to continue to support a mission that protects citizens, critical information, and even national security online. Many jobs in cybersecurity offer rewards that are similar to the military experience, such as the ability to thwart adversaries, make quick decisions in dynamic situations, and help defend the country.

Veterans are likely ahead of their civilian counterparts when it comes to preparing for a career in cybersecurity:

- Veterans were exposed to security procedures in the military and were trained to tackle challenges in a timely and systematic fashion.
- Veterans may have already acquired a security clearance during service, which can help when competing for a federal position, as well, as speed up the on-boarding process.

The demand for cybersecurity professionals is growing. There will be an estimated global cybersecurity **workforce shortage of 1.8 million by 2022**[1], making cybersecurity **one of the most in demand careers in the country**. In addition, cybersecurity professionals report **a median salary of $95,510—that's nearly three times the national average**[2]. This Guide will provide Veterans with the right tools and resources to obtain a high-paying, high-demand cybersecurity career.

The Department of Homeland Security (DHS) is committed to helping ensure our nation has a dependable workforce of skilled cybersecurity professionals. To support this goal, DHS is offering training and education resources to U.S. Veterans.

---

[1] (ISC)²™ Cybersecurity Workforce Study, 2017

[2] Bureau of Labor Statistics, 2017.

How Veterans transition to a new career after military service

Cybersecurity offers many different types of jobs in various environments. You might defend a network, create organizational strategies, or even try to breach systems to test vulnerabilities.

Veterans can take advantage of **free cybersecurity training and scholarship opportunities** to learn the knowledge, skills, and abilities (KSAs) needed to enter the cybersecurity field.

Short-term Plan

The very nature of cybersecurity is reacting to fast-paced evolving threats and vulnerabilities to our Nation's information systems. Familiarity with these threats can set Veterans apart during the job interviewing process. Certifications are industry-recognized validations of specific skills or experiences in a particular subject area. Employers often use certifications as a way to identify people with specific skill sets. Certifications help you stand out in a competitive job market. Fortunately, DHS provides training courses through the Federal Virtual Training Environment (FedVTE) platform with courses ranging from general security awareness and online user safety to highly technical advanced certifications.

Federal Virtual Training Environment (FedVTE)

DHS and Hire our Heroes (HOH) teamed up to provide Veterans access to FedVTE, **a free, online cybersecurity training center**. With 24/7 on-demand access to 60+ courses in varying levels of proficiency from beginner to advanced, Veterans can explore and take courses at their own pace. All courses align with the National Institute for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, allowing Veterans to build the necessary Knowledge, Skills, and Abilities (KSAs) to enter confidently into the cybersecurity workforce.

FedVTE delivers cutting-edge training courses, executive-level training, and industry certification preparation courses. You must adhere to each individual certification provider's requirements, including meeting experience requirements and paying any applicable fees. In a 2017 report, "after developing new skills from acquiring certifications or other training, survey respondents reported a 9 to 16% pay raise[3]."

[3] Global Knowledge, 2018

FedVTE FEDERAL VIRTUAL TRAINING ENVIRONMENT

Popular Cybersecurity Certifications

1. CompTIA Security+
2. E-C Council Certified Ethical Hacker (CEH)
3. CompTIA Network+ Certified Information Security Manager (CISM)
4. (ISC)^{2TM} Certified Information Systems Security Professional (CISSP)
5. CompTIA A+

There are many entry points into a cybersecurity career; the graphic below depicts one suggested track for newcomers that leverages existing free FedVTE training. Keep in mind when you successfully complete courses in the system, you will receive a FedVTE course completion certificate.

Beginner
0-3 years experience

Baseline IT Knowledge
CompTIA A+ Certification Prep.
CompTIA Network+ Certification Prep

Cybersecurity Concepts
101 Coding
101 Critical Infrastructure Protection
101 Reverse Engineering
Cybersecurity Overview for Mangers
Cybersecurity Risk Management for Managers
CompTIA Security+ Certification Prep
(ISC)^{2TM} Systems Security Certified Practitioner

Intermediate
3-5 years experience

(ISC)^{2TM} Systems Secure Software Lifecycle Professional (CSSLP)
Mobile and Device Security
Wireless Network Security (WNS)
Windows Operating System Security

Advanced Specialties
5+ years experience

CompTIA Security Practitioner Prep
Certified Ethical Hacker (EC-Council)
ISACA Certified Information Security Auditor (CISA)
ISACA Certified Informational Security Manager (CISM)
IPv6 Security
Linux Operating System Security
(ISC)^{2TM} Certified Authorization Professional (CAP)

Expert
5+ years experience

(ISC)^{2TM} Certified Information System Security Professional (CISSP) Certification Prep

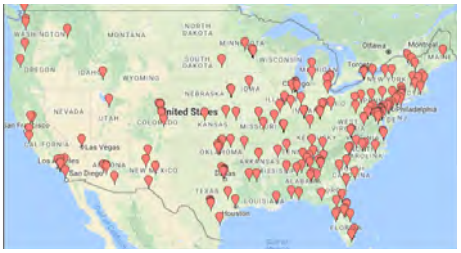
Optional Concentrations
(ISC)^{2TM} CISSP Concentration: ISSAP (Architecture)
(ISC)^{2TM} CISSP Concentration: ISSEP (Engineering)
(ISC)^{2TM} CISSP Concentration: ISSMP (Management)

Homeland Security

Long-term Plan

Certifications are a great way to quickly make job applicants more competitive to employers, but many cybersecurity careers also require a cybersecurity-related degree. The list below details general educational expectations in the cybersecurity field. Some employers may also look for advanced training, industry certifications, or work experience.

- **Associate's Degree**: Certain entry-level cybersecurity positions may be obtainable with a two-year associate's degree in computer science, cybersecurity or a related field, plus work experience.
- **Bachelor's Degree**: Plan on obtaining a four-year degree to compete for most cybersecurity jobs. A bachelor's degree in computer science, information technology, engineering, or a related discipline can be a good start.
- **Master's Degree**: Some employers hiring for cybersecurity positions may require candidates to have an advanced degree, such as a Master of Science in cybersecurity, information assurance, or a related field. An advanced degree typically takes an additional two years beyond the bachelor's level.



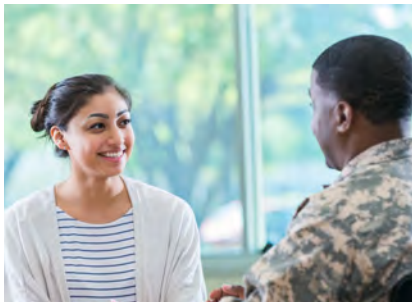
Designated Cybersecurity Schools: The National Centers of Academic Excellence (CAE) program, jointly supported by DHS and the National Security Agency (NSA), recognizes certain institutions and their outstanding cybersecurity-related degree programs with CAE designations. The curricula in these programs map to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.

CAE institutions offer cyber-related degree programs at community colleges, and at four-year colleges and universities. Program graduates often develop into cybersecurity experts who help to protect national security information systems, commercial networks, and critical information infrastructure in the private and public sectors. To learn more about the CAE program, visit https://niccs.us-cert.gov/education/national-centers-academic-excellence-cae.

Scholarships: The CyberCorps® : Scholarship for Service (SFS) program, co-sponsored by DHS and the National Science Foundation (NSF), offers cybersecurity scholarships to outstanding undergraduate, graduate, and doctoral students. Students can currently receive up to $34,000 to attend a participating institution.

SFS scholarships may fully fund the typical costs incurred by full-time students attending a participating institution, including tuition and related fees for up to two years. **Combine this with your GI bill and you might end up earning a cybersecurity degree for free!** There are currently 70+ institutions that receive SFS scholarship awards. To learn more about the SFS program, visit https://niccs.us-cert.gov/formal-education/cybercorps-scholarship-service-sfs.

Financial Assistance



Financial assistance is available through a variety of programs and websites outside of DHS. Below are some of the common financial assistance programs Veterans have access to.

- Yellow Ribbon Program
- GI Bill
- Tuition Assistance (TA) Top Up
- Vocational Rehabilitation
- Community College Cyber Pilot Program

Additionally, Veterans may receive tuition discounts at some colleges and universities.

National Initiative for Cybersecurity Careers and Studies (NICCS)

In addition to FedVTE, DHS developed the NICCS Education and Training Course Catalog, an open source tool to help aspiring and current cybersecurity professionals locate nearby cybersecurity-related courses. With more than 4,000 courses (and growing) aligned to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, users can easily filter to find modules that are appropriate to their interest and level of professional development.

Veterans can visit the Course Catalog to find their next cybersecurity-related course quickly.

Remember, the Post-9/11 GI Bill, is worth up to 36 months of financial support for education and training for graduate and undergraduate degrees, vocational/technical training, correspondence training, licensing and national testing programs, and tutorial assistance to prepare you for a career in cybersecurity.

What Jobs Are Out There?

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework provides common language on cybersecurity roles and helps define professional requirements. The NICE Cybersecurity Workforce Framework organizes cybersecurity into **seven high-level categories**, each comprised of several specialty areas.

This organizational structure is based on extensive job analyses that groups together work and workers that share common major functions, regardless of job titles or other occupational terms. The NICE Cybersecurity Workforce Framework includes many categories of work Veterans might find familiar from having a military background.

While technical expertise is sought after, not all cybersecurity work opportunities require deep technical expertise – there is a strong need for individuals with experience and skills in program management, people management, policy development, and training.

For example, when exploring Categories like **Oversee and Govern** and **Operate and Maintain** there are less technical roles:

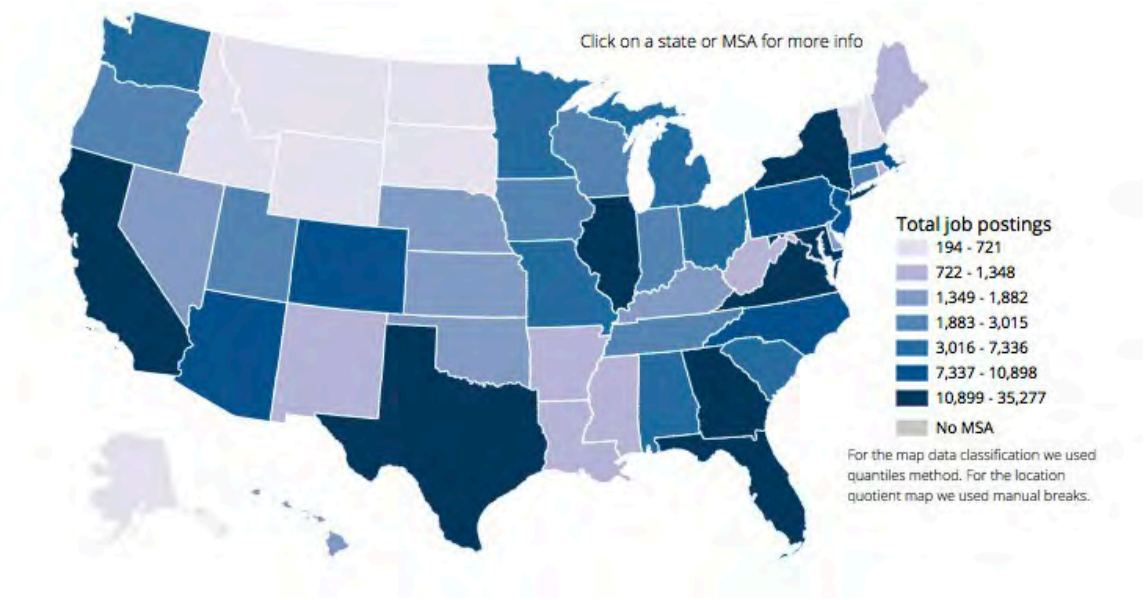
- **Education and Training**: developing, planning, and delivering training on cybersecurity subjects
- **Strategic Planning and Policy Development**: defining strategy and policy direction as it pertains to cybersecurity standards and operations
- **Knowledge Management**: managing, organizing, and securing access to information
- **Data Administration**: developing and administering databases that allow for the storage, query, and utilization of data

Exploring the categories and specialty areas of the NICE Cybersecurity Workforce Framework shows the wide range of options available while preparing to launch a new and exciting career in cybersecurity. Additionally found in the Framework are capability indicators, which provide an understanding of the qualities or accomplishments that cybersecurity professionals possess across proficiency levels, and signal a greater likelihood of success in each work role.

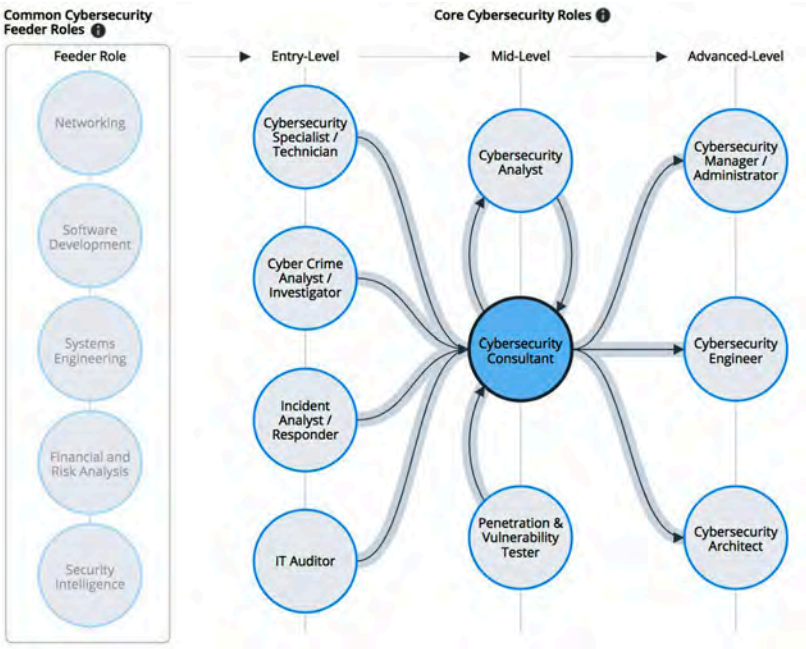
Veterans are encouraged to explore the NICE Cybersecurity Workforce Framework on the National Initiative for Cybersecurity Careers and Studies (NICCS) website. NICCS hosts an interactive framework tool allowing individuals to browse and evaluate how their skills fit into the cybersecurity workforce. NICCS also serves as a national resource for cybersecurity awareness, education, training, and career opportunities. NICCS makes training information available through a robust, searchable catalog which allows users to find cybersecurity training programs based on location, preferred delivery method, specialty area, or proficiency level.

Cyberseek.org

Cyberseek.org provides a variety of tools to locate supply and demand of cybersecurity jobs, interactive career pathways mapped to the NICE Cybersecurity Workforce Framework, top job titles, key jobs within cybersecurity and transition points between jobs, salaries, credentials, and skillsets associated. Click on the map to go directly to the Cybersecurity Workforce Heat Map to get a better understanding of the jobs in your state or local area.



Military experience may help pave the way to a cybersecurity career. Many companies prefer to hire Veterans for cybersecurity positions because of the training Veterans received in the military. Additionally, some work may require navigating systems and tracking down persistent threats: skills Veterans may have gained through military service. Click on the Career Pathway graphic to explore various roles and positions and find out how to advance within the field.



> *Cybercrime categorically ranks with drug trafficking as a worldwide economic danger.*[3]

For Employers

On behalf of DHS, we would like to thank you for your help in reaching out to our nation's Veterans. We are excited to offer these resources to those who have served and are interested in launching a cybersecurity career.

DHS also offers a variety of ways to get started promoting free cybersecurity training to Veterans. From sample blogs and social media posts to downloadable materials, DHS has you covered.

DHS offers ready-to-use messaging for your Veteran members. Copy and paste the sample messages into an email, social media post, or blog and share it with your network.

To get started, visit our Veterans Training page on NICCS. Refer to the Champions Communications Manual for sample language and templates.

Partner with us

Send us an email at Cybersecurityworkforce@hq.dhs.gov to share upcoming events or find out about other opportunities.