Veterans User Guide

Publication: March 2024
Cybersecurity and Infrastructure Security Agency

NICCS VETERANS USER GUIDE

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 is currently an estimated global cybersecurity workforce shortage of 3.4 million[1] making cybersecurity one of the most in demand careers in the country. In addition, cybersecurity professionals report a median salary of $112,000—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 Cybersecurity and Infrastructure Security Agency (CISA) is committed to helping ensure our nation has a dependable workforce of skilled cybersecurity professionals. To support this goal, CISA is offering cybersecurity-related training, education, and career resources to U.S. Veterans.

[1] (ISC)[2] Cyber Workforce Study, 2023.
[2] Bureau of Labor Statistics, 2023.

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 Workforce Framework for Cybersecurity (NICE 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.

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.

Popular Cybersecurity Certifications

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

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 in Cybersecurity (NCAE-C) jointly supported by DHS and the National Security Agency (NSA), recognizes certain institutions and their outstanding cybersecurity-related degree programs with NCAE-C designations. The curricula in these programs map to the NICE Framework.

NCAE-C 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. Learn more about the NCAE-C program.

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 $27,000 to $37,000 for undergraduate and graduate studies at participating institutions.

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 400+ institutions that receive SFS scholarship awards. Learn more about the SFS program.

Financial Assistance

Veterans may receive tuition discounts at some colleges and universities. Financial assistance is available through a variety of programs and websites outside of CISA. 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

National Initiative for Cybersecurity Careers and Studies (NICCS) website

The National Initiative for Cybersecurity Careers and Studies website, commonly referred to as NICCS, is a one-stop-shop for cybersecurity-related education, training, and career information including the NICCS Education and Training Catalog. With more than 13,000 courses (and growing) aligned to the NICE Framework, users can easily filter to find modules that are appropriate to their interest and level of professional development. With in-person and virtual options for beginner, intermediate, and advanced users, NICCS truly has something for everyone! Veterans should visit the NICCS Education & Training Catalog to find their next cybersecurity-related course to help them advance their career.

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?

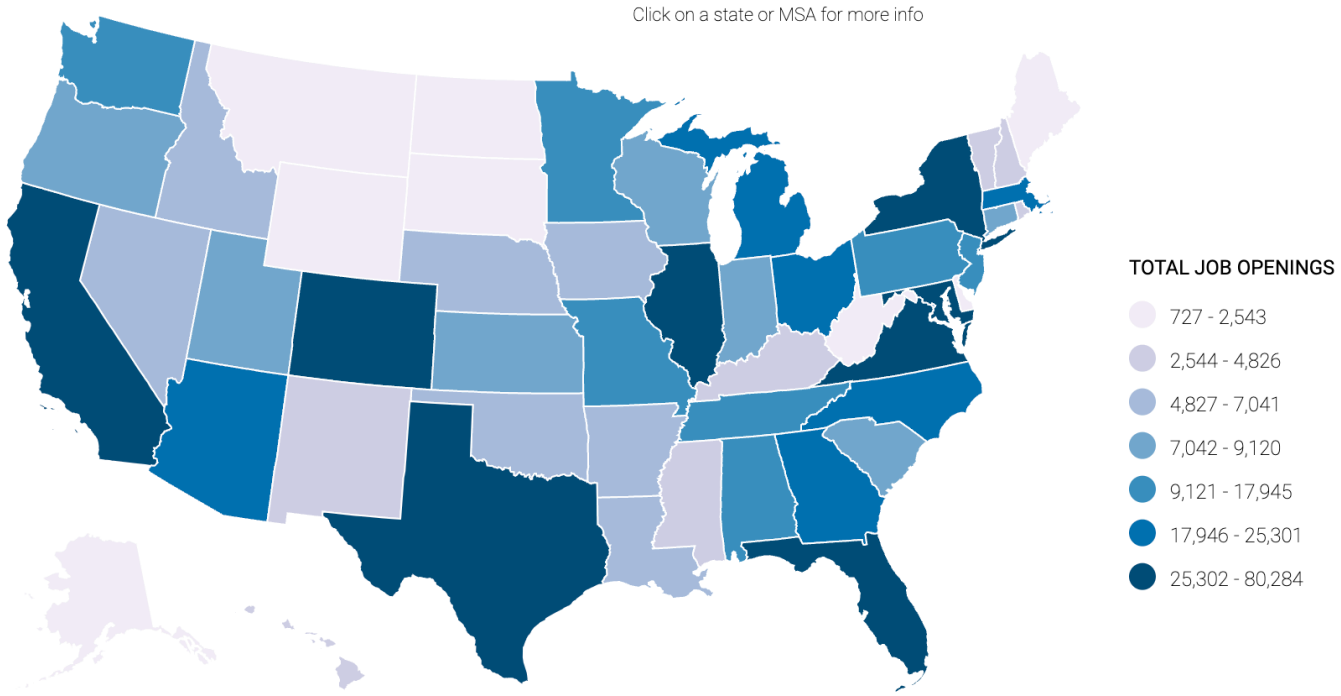
The NICCS website hosts interactive tools to help current and prospective cybersecurity professionals, including Veterans transitioning out of the Military, find cyber-related career options that align with their knowledge and skills such as the Cyber Career Pathways Tool and the Interactive Cybersecurity Career Map.

The Cyber Career Pathways Tool helps users identify, build, and navigate a potential cyber career pathway by increasing your understanding of the knowledge, skills, and abilities needed to begin, transition, or advance your cyber career. It depicts the Cyber Workforce according to five distinct, yet complementary, skill communities. The Tool also highlights core attributes among each of the NICE Framework's 52 work roles and offers actionable insights for employers, professionals, and those considering a career in cyber.

The Interactive Cybersecurity Career Map shows thousands of open federal cybersecurity positions in CISA and other federal agencies across the country and around the world. Select an area on the map or search by keyword, salary range, and location to find an open position that can help improve career opportunities.

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.

For Employers

On behalf of CISA, 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.

CISA also offers a variety of ways to get started promoting free cybersecurity training to Veterans. CISA offers ready-to-use

messaging for your Veteran members – from sample blogs and social media posts to downloadable materials. Copy and paste the sample messages into an email, social media post, or blog and share it with your network. CISA has you covered!

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

PARTNER WITH US

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