Frequently Asked Questions

NICE and our community:

- Q: What is NICE?
- A: NICE is the National Initiative for Cybersecurity Education. We are headquartered in Gaithersburg, MD and our work focuses on efforts to close the hiring gap in the cybersecurity workforce. We are led by the National Institution of Standards and Technology (NIST) in the U.S. Department of Commerce, and are a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Visit our about page for more information.

- Q: How can I get involved with NICE?
- A: There are many ways to get involved. You can attend our events – the NICE Conference & Expo is held annually typically in early November and the NICE K12 Cybersecurity Education Conference is held annually in early December. The NICE Program Office also hosts free webinars as well as monthly working group meetings. You can also help us celebrate National Cybersecurity Career Awareness Week each year in the second week of November.

- Q: How do I join the NICE Community?
- A: Our NICE Working Group and subgroups are the most active way to join the NICE Community. All groups meet virtually by teleconference and web meeting. We would welcome your participation. Visit the NICE Working Group website for more information.

- Q: How do I get in contact with NICE?
- A: Please email us at: nist.nice@nist.gov.

NICE and you:

- Q: What is the NICE Cybersecurity Workforce Framework?
- A: The NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181, is a national-focused resource that categorizes and describes cybersecurity work. Visit the NICE Framework website for more information about the NICE Cybersecurity Workforce Framework including a copy of the publication and tools and resources for implementing and using it.

- Q: Will the NICE Framework be updated and how can I provide input?
- A: The NICE Framework is a living document that will be updated periodically based on change requests to the NICE Program Office. NICE will consider recommendations (change requests) for expansion, update/correction, withdrawal, or integration of NICE Framework components using the process described on the NICE Framework Revisions web page.

- Q: What is the difference between the NICE Framework and the Cybersecurity Framework?

- A: The Cybersecurity Framework or Framework for Improving Critical Infrastructure Cybersecurity (currently version 1.1) is a voluntary framework consisting of standards, guidelines, and best practices to manage cybersecurity-related risk [the *how* and *what* of cybersecurity]. The NICE Cybersecurity Workforce Framework (see question above) describes and categorizes roles and functions [the *who* of cybersecurity]. Read more about connections between these two frameworks in an article featured in the NICE enewsletter.

- Q: What is CyberSeek?
- A: CyberSeek is a cybersecurity career "heat map," providing detailed, actionable data about supply and demand in the cybersecurity job market. CyberSeek also features a career pathway tool that maps opportunities for advancement in the cybersecurity field. The information in the map and pathway align with the NICE Cybersecurity Workforce Framework. CyberSeek was developed by CompTIA in partnership with Burning Glass Technologies under a grant from NICE.

- Q: Where can I learn more about cybersecurity jobs and careers?
- A: Please reference the National Cybersecurity Career Awareness Week for more information.

- Q: Where can I find a list of the "appropriate industry recognized certifications" that have been identified by NICE as mentioned in the Cybersecurity Workforce Assessment Act?
- A: Please see this list, which is compiled from current course listings in the Department of Homeland Security NICSS Education and Training Catalog. The course catalog provides a list of courses that are aligned to the specialty areas of the NICE Cybersecurity Workforce Framework. Our NICE Working Group Training and Certifications Subgroup is also working on a mapping of certifications to the NICE Framework.

Career and educational topics:

- Q: What kind of education or skills should I have or do I need to get a cybersecurity job/career/degree/etcetera?
- A: Cybersecurity education can be acquired in a variety of ways. Check your local community college or university to see if they have cybersecurity courses or programs. The CyberSeek pathway tool presents a sample of cybersecurity jobs with information about certifications, skills, and degree levels commonly required for the job. Hands-on experience is increasingly important.

- Q: Where can I get said education/skills?
- A: The Center of Academic Excellence (CAE) Community can be a great place to start if you're looking for formal education programs at two- and four-year institutions. There are also many online training programs or Massive Open Online Courses (MOOCs), bootcamps or other "crash course" training programs provided by certification providers, and apprenticeship programs.

- Q: Is getting certain or a lot of certifications better than getting a degree?

- A: This varies from employer to employer. CyberSeek shows that the majority of employers prefer at least a Bachelor's degree. See also the NICE One Pager on the Value of Certifications.

- Q: Are there scholarships available?
- A: Here are a few scholarships specific to studying cybersecurity, some may be restricted to specific demographics so please review the information on each. Set up a search engine alert on scholarships to remain aware of new programs or pending deadlines for applying:
    - Computing Research Association Scholarships for Women Studying Information Security
    - CyberCorps: Scholarship for Service (SFS)
    - DoD Cybersecurity Scholarship Program (formerly known as Information Assurance Scholarship Program – IASP)
    - Exabeam Cyber Security Scholarship
    - ISC(2) Graduate Scholarship, Women's Cybersecurity Scholarships
    - ISSA Education Foundation Scholarship
    - SANS VetSuccess Academy, Women's Academy, Cyber Workforce Academy, and Diversity Cyber Academy
    - Snort Scholarship
    - Warrior to Cyber Warrior Veteran Training Program

Building your career:

- Q: How can I build hands-on skills and gain experience?
- A: Participating in cybersecurity related competitions, job shadowing a cybersecurity professional, volunteering in your community, and doing cybersecurity research or being self-taught all relate to job experience. Internships both in cybersecurity-specific roles and in "feeder roles" such as network management and IT help desk can help you gain important experience and skills. Apprenticeships are increasingly available in both cybersecurity areas and in these "feeder roles."

- Q: What else can I do to be job-ready?
- A: Employers often mention the importance of "soft skills" like communication and presentation-skills for a cybersecurity professional. NICE has a webinar devoted to this issue and tutorials on resume-writing and interview techniques.

- Q: How do I network or connect with potential employers?
- A: A good way to connect with possible job employers is to visit your local or community technology organizations such as ICMCP, InfraGard, ISACA, ISSA, TECNA, and DefCon, The National Cybersecurity Student Association, OWASP, etcetera.Use social media such as LinkedIn to identify practitioners in your community and request a connection or suggest an "informational interview" to learn more about their role and career. You can also visit employer's websites and look at their career section to spot open positions.

- Q: I have a degree in cybersecurity but am having trouble finding a job. What can I do to increase my chances?

- A: First, examine your resume to be sure it properly highlights your skills and experience, not just your classes and degree. Next, get feedback on your resume and interviewing skills to eliminate either of those activities as holding you back. Great places for feedback are from professionals in the field; people you may know from industry groups or even professionals online who are willing to help mentor job seekers. It doesn't hurt to ask for help. Check social media for groups where discussions like this are plentiful.

  Many professionals report that it was only when they added a few industry-recognized certifications to their resume, in addition to their degree and some demonstrated real-world experience, that the offers came in. Set up an in-home lab so you can practice what you learn in the classroom; volunteer your time with community organizations who would benefit from your knowledge; stay current on the latest threats by signing up for alerts and newsletters.

Miscellaneous:

- Q: I'm a veteran. How do I translate my skills, knowledge, and experience to civilian cybersecurity roles?
- A: Remember to translate your important military and cybersecurity training and experience to "civilian-speak." Use the O*Net tools to find equivalent terminology for your resume. Military.com has MOS (Military Occupation Specialty) mapping. The My Next Move website can help identify how a military person might describe their work and provides examples. The FedVTE provides free online cybersecurity training for US Government personnel and veterans. Career sites like LinkedIn may have specialty areas for veterans. Many employers and training programs have developed veteran-focused hiring programs; here is a sampling:
  - Bank of America Military Affairs
  - Cisco Veterans Program
  - Dell Military and Veterans
  - Fortinet's Fortivet program
  - IBM Veterans Employment Initiative
  - Microsoft Military Affairs
  - Raytheon Operation Phoenix Program
  - SANS VetSuccess Academy
  - Wells Fargo Military Veterans
  - Warrior to Cyber Warrior Veteran Training Program

- Q: I don't have a security clearance, can I work in cybersecurity?
- A: Not all cybersecurity jobs require a clearance, but many do. Most roles in the private sector do not require security clearances but those with sensitive government-related work might. Employers sponsor clearances and for a candidate with the right background and experience, their lack of a clearance will not be an issue; it just may require time to get the desired approvals.

- Q: How do I get a security clearance and what is its purpose?
- A: For more information, please watch this NICE Webinar: Shedding Light on Security Clearances - Process, Requirements, and Considerations.

Still have questions? Email us at nice.nist@nist.gov.