NIST NICE Request for Information
Next Gen Cyber Foundation

General Information

1. Are you involved in cybersecurity workforce education or training (*e.g.*, curriculum-based programs)? If so, in what capacity (including, but not limited to: Community college or university faculty or administrator; official with a non-profit association focused on cybersecurity workforce needs; manufacturer or service company that relies on cybersecurity employees; cybersecurity curriculum developer; cybersecurity training institute; educator in a primary grade school; government agency that provides funding for cybersecurity education; or student or employee enrolled in a cybersecurity education or training program)? *Note:* Providing detailed information, including your specific affiliation is optional and will be made publicly available. Commenters should not include information they do not wish to be posted (*e.g.*, personal or confidential business information) and are strongly encouraged not to include Personally Identifiable Information in their submissions.

Yes, Next Gen Cyber Foundation is an upcoming non-profit organization—to be launched 1st quarter of 2018—promoting cybersecurity careers and workforce development. The leadership team is comprised of cybersecurity industry leaders and entrepreneurs, employers, workforce development experts, college professors, and practitioners. The foundation will provide career counseling and mentorship to new and aspiring cybersecurity professionals, transitioning military service members, career changers, and students. We strive for successful careers in cybersecurity accessible to all people regardless of demographic and socioeconomic status.

Leadership:

Regine Bonneau, *JD/JSM, MBA, BBA*
Chairman, Board of Directors, Next Gen Cyber Foundation
Current Position: Founder and CEO, RB Advisory LLC

William McBorrough, *MSIA, CISSP, CISA, CRISC, CEH, HITRUST CSFP*
Member, Board of Directors, Next Gen Cyber Foundation
Current Position: Co-Founder and Managing Partner, McGlobal Tech, Founder and President, Next Gen Cyber LLC, Adjunct Professor, Cybersecurity, University of Maryland University College

Thuy Truc To, *MS, High Technology Criminal Investigation, BS, Information Systems, Security+ CE*
Executive Director, Next Gen Cyber Foundation
Current Position: SME II Incident Management Support, Copper River Enterprise Services

Youlanda Burress, *MS, Health Administration/Health Care Ethics, BA, Global Management and Commutation*
Chief Financial Officer, Next Gen Cyber Foundation
Current Position: Program Analyst, U.S. DOS

Felice Flake, *Candidate, MBA, Information Security Management, MS, Cybersecurity, BA, Criminal Justice—Homeland Security, Security+CE*
Chief Technical Officer, Next Gen Cyber Foundation
Current Position: Founder and CEO, ScySec LLC

Mission Statement:
Our mission is to become a global advocacy organization for Cybersecurity Workforce Development.

Vision:
Our vision is to provide support and resources to:

- increase cybersecurity and cybersecurity career awareness
- guide individuals in starting or transitioning into their new cybersecurity careers and advancing their careers
- guide organizations in building quality and effective cybersecurity programs

Values:

- Accessible and Inclusive - We strive to make our programs and services accessible to everyone because we recognize that in order to have a strong cybersecurity workforce, it will involve everyone from all demographics.
- Integrity - We remain true to our mission to provide quality programs and services to all.
- Respect - We treat everyone with dignity and respect.
- Ambition - We strive always to improve our programs and services as the cybersecurity field continues to evolve.
- Common sense - We will not succeed in protecting our data without it.

If you would like to inquire more about Next Gen Cyber Foundation, please visit us at www.nextgencyberfoundation.org or contact info@nextgencyberfoundation.org.

Growing and Sustaining the Nation's Cybersecurity Workforce

1. What current metrics and data exist for cybersecurity education, training, and workforce developments, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

"In 2015, Frost & Sullivan forecasted a 1.5 million worker shortage by 2020. In light of recent events and shifting industry dynamics, that forecast has been revised to a 1.8 million worker shortage by 2022. This is reflected by the extraordinarily high number of professionals across the globe who indicate that there are not enough workers in their departments." (Frost & Sullivan, 2017) The metrics from the Frost & Sullivan report must be analyzed and its significance recognized as the response to the cybersecurity education and training questions are reviewed.

Some of the current metrics and data reside with the professional organizations and certifying authorities like ISC^2, ISACA, CompTIA, and SANS Institute. Other professional organizations related to cyber security, information security, and IT security include IAPP (International Association of Privacy Professionals) and EC Council. There is also data related to higher education and the degrees related to information technology, cyber security, and data security. Higher education provides similar training to that of training providers who offer exam preparation along with intensive technical training.

"$(ISC)^2$ is an international, nonprofit membership association for information security leaders like you. We're committed to helping our members learn, grow and thrive. More than 125,000 certified members strong, we empower professionals who touch every aspect of information security." ((ISC)2.org, 2017)

"ISACA provides practical guidance, benchmarks and other effective tools for all enterprises that use information systems. Through its comprehensive guidance and services, ISACA defines the roles of information systems governance, security, audit and assurance professionals worldwide. The COBIT framework and the

CISA, CISM, CGEIT, and CRISC certifications are ISACA brands respected and used by these professionals for the benefit of their enterprises." (ISACA.org, 2016)

"International Council of E-Commerce Consultants, also known as EC-Council, is the world's largest cyber security technical certification body. We operate in 145 countries globally[,] and we are the owner and developer of the world-famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (C|HFI), Certified Security Analyst (ECSA), License Penetration Testing (Practical) programs, among others." (ECCouncil.org, 2017)

"IAPP, or the International Association of Privacy Professionals…is the largest and most comprehensive global information privacy community and resource, helping practitioners develop and advance their careers and organizations manage and protect their data." (IAPP.org, 2017)

2. Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

In some organizations, there is sufficient understanding and agreement about workforce categories while in other organizations our team is receiving anecdotal evidence that human resources personnel is wielding too much power over the hiring process.

In one situation, the credentialed candidate was contacted by the hiring manager and asked to apply on the company website for a particular position. The position was middle management but set the hiring manager and organization up for having someone onboard who was experienced in the multiple projects planned by the Information Technology/Information Security leadership team. When the human resources director contacted the candidate, they questioned the candidate about why they wanted the position. It was unfortunate for the company because their HR Director was more focused on his power and failed to consult with the hiring manager about the candidate. This example is not indicative of all human resources professionals but a lack of understanding the organizational requirements—especially for cyber security—hinders the success of the internal teams.

Individual stories vary, but there is a common thread among them—the use of applicant tracking systems is convenient, yet it can be harmful to the overall process of hiring suitable candidates for IT/IS positions. It is imperative to have human resources professionals working closely with the IT/IS leaders in determining necessary skill sets and experience level. Also, organizations need to realize there is not a perfect demographic but rather all demographic groups can be advantageous for their team.

There is quite a bit of media attention being placed upon the cybersecurity skills gap. Our team is aware of highly qualified candidates who are being dismissed because they are over the age of forty. Again, this is just one symptom of the self-perpetuating deterrents to reducing the cyber skills shortage. The focus should shift to tiers of expertise and credentials as the first level, some experience and education or training as the second tier and third tier can be modeled on an apprenticeship model.

3. Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

Yes, our foundation is building our infrastructure to serve both operability and security at every juncture in our organizational development. We will continuously review and implement best practices based on NIST documents. Members of our leadership team are actively involved in other professional organizations and initiatives which serve to strengthen our organization through actions that affirm our commitment to being lifelong learners.

4. What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (*e.g.*, energy vs financial sectors)?

Many employers are hyper-focused on certifications such as the $(ISC)^2$ CISSP and the ISACA CISM and CISA. All three of these are intensive certifications and require authentication of the years of experience in conjunction with the actual certification exams. The habit of HR professionals often focusing too much on one set of requirements is causing potential harm to the overall hiring process for security personnel. For example, many traditional universities have developed comprehensive information technology and cyber security programs which also include courses in other areas related to traditional business and management requirements. Employers, their HR teams, and even their IT/IS teams must work together to develop elasticity in hiring based on education, experience, and certifications. There does not need to be necessarily be all three for entry and mid-level positions, but applicants need to be interviewed and considered as hired in possibly a tiered manner based on the scope of their qualifications.

Other certifications which are highly sought after as they are quite comprehensive in their exam questions. However, negative repercussions are surrounding these certifications. The high cost of exams is a source of great stress and financial strain for many participants.

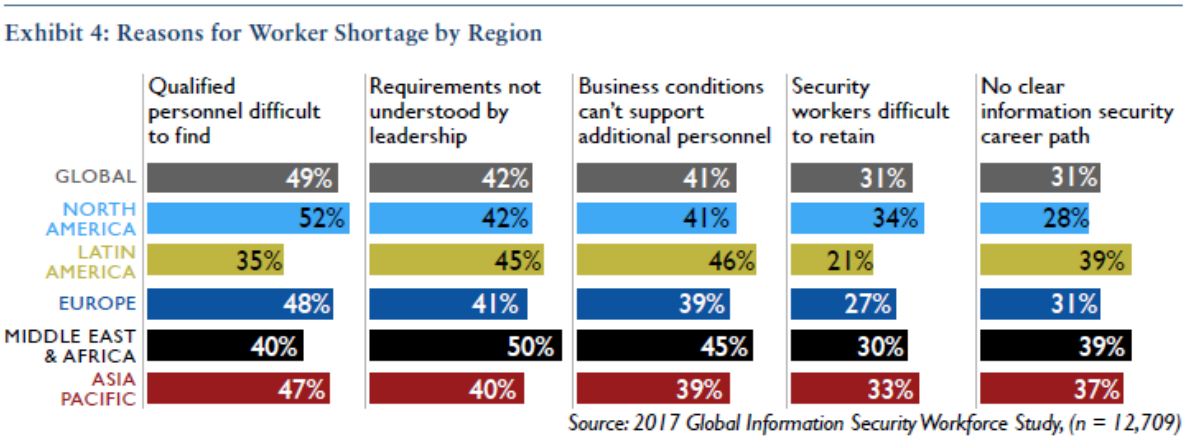
5. Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

Many private training companies charge high fees for training classes. Many of them offer boot camps which can be highly lucrative for their businesses but are not always the best option for their customers. One of the most effective training programs is delivered by the SANS Institute. They offer numerous training programs, and several of them work in conjunction with their graduate level degree and certificate programs.

Other highly efficient sources of cybersecurity education are offered by several universities across the United States. “The Department of Homeland Security (DHS) and the National Security Agency (NSA) jointly sponsor the National Centers of Academic Excellence (CAE) program. Specific 2 and 4-year colleges and universities are designated based on their robust degree programs and close alignment to specific cybersecurity-related knowledge units (KUs), validated by top subject matter experts in the field.” (National Centers of Academic Excellence (CAE), 2017)

6. What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

For employers, it is making certain their human resources, and IT/IS leaders have clarity that there is not a perfect recipe for many of the open positions. Being a CISSP, CISM, or CISA, does not guarantee the candidate is going to be the most qualified. It is tedious to consider the extensive interviewing, but the wrong assessments are being used in most interviews. The overhaul of the system, ironically, requires HR to move away from overreliance on Applicant Tracking Systems (ATS). The inclusion of all applicants—no matter what age, race, culture—need to be viewed as potential employees who make the team better. Training these employees will require some IT/IS teams to rethink their culture and jobs. Side-by-side training is a successful training strategy, but the IT/IS culture often over focuses on the sense of competitiveness rather than nurturing non-traditional new team members.



(Frost & Sullivan, 2017)

Some of the more troubling data in the above table related to the "Requirements not understood by leadership" and this is a critical issue. The skill shortage is aggravated by the lack of leadership's understanding of the organizational need since leaders make the decisions related to budgeting. This practice has a domino effect on the entire organization with regard to risk management.

In the 2016 book, *Women in Security: A Practical Guide for Career Development,* the following illustration of some leaders' attitudes toward security was described:

> "[A] conference predominantly attended by women and the panel of women leaders were each impressively credentialed and experienced. It was a moderately large group and it was not necessarily focused on just information security, IT security, and cybersecurity but rather IT overall. When the panel was questioned about their positions on security in their organization, two of the three panelists were dismissive of the importance of security and explained their leadership role did not include security policies.
>
> Lack of support for information security, IT security, and cybersecurity policies is a huge part of the problem for security professionals—entry-level to highly experienced—in both the public and private sectors. There is some of the stereotypical machismo but…it is equally balanced with strong, secure male security professionals who welcome women into the profession. The demographic of support crosses generations and cultures, common personality traits include strong leadership skills and an appreciation of individual contributions in a team setting." (Davies, 2016)

Some professionals rely strictly on the certification route, and this choice serves them quite well. Other professionals pursue their undergraduate degrees in computer science- or information technology-related fields then choose a certification which can act as a complement to their formal education. There are overlaps in the training content, and the challenge is considering the requirement for certifications which are often cost prohibitive. Student loans can be obtained for higher education undergraduate and graduate degrees, but there is not necessarily a mechanism other than private loans for those individuals who prefer to pursue intensive certification courses through $(ISC)^2$ or SANS Institute.

7. How will advances in technology (*e.g.*, artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

"What used to be the stuff of science fiction has turned into reality. No longer do we dream of a world where devices around us are interconnected, share information with one another, and carry out actions autonomously — we are now living in it, thanks to the so-called Internet of Things (IoT). Such new technology holds great potential to make our lives easier, more convenient, and more comfortable, but new technology always comes with new — and very real — security threats. Already, we have observed ransomware infecting smart TVs, connected cars being remotely controlled by hackers, and internet protocol cameras becoming cyber weapons in massive distributed denial-of-service attacks." (Change, 2017)

The advances in technology (e.g. artificial intelligence, Internet of Things, etc.) offer end users a tremendous amount of convenience. It is appealing and exciting for tech-savvy customers to be able to access their home remotely but many individuals do not consider the security risks inherent to increasing their access and convenience. The increase in the attack surfaces requires additional security personnel for support and monitoring.

"2016 brought a long-feared DDoS threat to fruition: Cyber attacks launched from multiple connected devices turned into botnets. A 665-Gbps attack targeted the security blogger Brian Krebs in September.22 Shortly thereafter, a 1-TBps attack was launched against the French hosting company OVH.23 And in October, DynDNS suffered an attack that caused an outage to hundreds of popular websites—the largest of the three Internet of Things (IoT) DDoS attacks.24
These attacks propelled us into the 1-TBps DDoS era. They shook traditional DDoS protection paradigms and proved that the IoT DDoS botnet threat is real—and that organizations must be prepared." (Cisco Systems, Inc., 2017)

As our global society grows more dependent on conveniences of technology, the risk of this technology must be managed through security solutions involving technology and security practitioners. The importance of balancing convenience and security must be emphasized in all education and training programs.

8. What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation's cybersecurity workforce, taking into account needs and trends? What steps should be taken:

i. At the Federal level?
At the federal level, one of the most impressive programs is the FedVTE. "Federal Virtual Training Environment (FedVTE) is a free online, on-demand cybersecurity training system that is available at no charge for government personnel and veterans. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis." (NICCS.US-CERT.gov, 2017)

Their site is already set-up to train veterans and requires the veteran to complete registration and verification process. To create a benefit for veterans and their families, the FedVTE should be offered to spouses of veterans as well. This effort could be coordinated through the FedVTE's managing division, the National Initiative for Cybersecurity Careers and Studies, or NICCS.

ii. At the state or local level, including school systems?

There are many schools already participating in the CyberCorps: Scholarships for Service program, but many more should be encouraged and possibly incentivized to take part in the program as well. [The Scholarships for Service program]…is the Federal Government's response to deal with the threat to our information technology infrastructure by strengthening the cadre of cybersecurity/information assurance professionals who protect it. Through this program, the National Science Foundation partnered with Department of Homeland Security issues selected 4-year colleges and universities scholarship grants to attract students to the [cybersecurity]/information assurance fields. The U.S. Office of Personnel Management administers the operational aspects of the program." (CyberCorps: Scholarship for Service, 2017)

Two important initiatives originated at Tennessee Tech University—the Cybersecurity Education, Research, and Outreach Center (CEROC) and the Women in Cybersecurity, or WiCys. "…Tennessee Tech Cybersecurity Education, Research, and Outreach Center (CEROC) was established in Summer 2015 with in an effort to integrate university wide existing activities and initiatives in cybersecurity education, research and outreach. In October 2015, we were designated as a National Center of Academic Excellence in Cyber Defense Education (CAE-CD) through the academic year 2021. NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA/CD programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines." (Tennessee Tech University, 2017)

"The WiCyS initiative was launched in 2013 with support from a National Science Foundation grant…WiCyS has become a continuing effort to recruit, retain and advance women in cybersecurity. It brings together women (students/faculty/researchers/professionals) in cybersecurity from academia, research and industry for sharing of knowledge/experience, networking and mentoring." (Women in Cyber Security, 2017)

These programs should be supported by other universities, training partners, and collaboration encouraged with professional associations. In many aspects, they serve as a template for building similar programs—even a modified version—at other universities and colleges.

iii. By the private sector, including employers?

Companies should support partnerships among the professional associations like SHRM (Society for Human Resources) and $(ISC)^2$, ISACA, ISSA, and IAPP. Comprehensive surveys of members along with joint events and panel discussions focused on developing hiring solutions should be encouraged. In conjunction with the professional association partnerships, local colleges and universities should be invited to join these events as there are multiple facets to the challenges faced by students entering the workforce, and those students who are making a career change.

iv. By education and training providers?

Education and training institutions should sign a pledge to adhere to specific ethical guidelines related to the various certification and exam prep courses. This document can be developed through collaboration among professional organizations, CEOs and VPs of training from the education and training providers, and security practitioners. Focusing on excellence and ethics supports the behavior required by security professionals at all levels.

v. By technology providers?

Some technology providers do offer scholarships to individuals interested in entering the cybersecurity field. “To help close this security skills gap, Cisco is introducing the Global Cybersecurity Scholarship program. Cisco will invest $10 million in this program to increase the pool of talent with critical cybersecurity proficiency. Cisco also has enhanced its Security certification portfolio with a new CCNA Cyber Ops certification. Through the scholarship program, Cisco will offer free training, mentoring, and testing designed to help you earn CCNA Cyber Ops certification and hone the skills needed for the job role of security operations center analyst. The new CCNA Cyber Ops certification has been designed to address the critical skills deficit, providing the job-ready knowledge needed to meet current and future challenges in network security.” (Cisco Systems, Inc., 2017)

Other technology providers should follow the example set forth by Cisco, and there should be partnerships forged with universities, training providers, and non-profit organizations so that information about such worthwhile programs can be shared with the greatest number of potential participants.

References

(ISC)2.org. (2017, July 25). *About Us*. Retrieved from (ISC)2.org: https://www.isc2.org/en/About

Change, S. (2017, July 31). *Expectations for Communication Service Providers on IoT Security*. Retrieved from IoT Security Headlines: https://www.trendmicro.com/us/iot-security/special/232

Cisco Systems, Inc. (2017). *Cisco 2017 Midyear Cybersecurity Report.* San Jose, CA: Cisco Systems, Inc.

Cisco Systems, Inc. (2017, July 31). *Expand Your Career Opportunities*. Retrieved from Cisco.com: https://mkto.cisco.com/Security-Scholarship.html

CyberCorps: Scholarship for Service. (2017, July 31). *CyberCorps: Scholarship for Service*. Retrieved from sfs.opm.gov: https://www.sfs.opm.gov/StudFAQ.aspx#num8

Davies, S. J. (2016). *Women In Security: A Practical Guide for Career Development, First Edition.* New York, NY: Elsevier.

ECCouncil.org. (2017, July 25). *About Us*. Retrieved from ECCouncil.org: https://www.eccouncil.org/about/

Frost & Sullivan. (2017, July 30). *2017 Global Information Security Workforce Study*. Retrieved from iamcybersafe.org: https://iamcybersafe.org/wp-content/uploads/2017/07/N-America-GISWS-Report.pdf

IAPP.org. (2017, July 26). *IAPP Mission and Background*. Retrieved from IAPP.org: https://iapp.org/about/mission-and-background/

ISACA.org. (2016, January 14). *About ISACA.* Retrieved from ISACA.org: http://www.isaca.org/about-isaca/Pages/default.aspx

National Centers of Academic Excellence (CAE). (2017, July 30). Retrieved from National Initiative for Cybersecurity Careers and Studies (NICCS.us-cert.gov: https://niccs.us-cert.gov/formal-education/national-centers-academic-excellence-cae

NICCS.US-CERT.gov. (2017, July 31). *Federal Virtual Training Environment (FedVTE)*. Retrieved from NICCS: National Initiative for Cybersecurity Careers and Studies: https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte

Tennessee Tech University. (2017, August 1). *CEROC: Cybersecurity Education, Research and Outreach Center*. Retrieved from TNTECH.edu: https://www.tntech.edu/ceroc/

Women in Cyber Security. (2017, August 1). *About Women in CyberSecurity (WiCyS)*. Retrieved from csc.tntech.edu: https://www.csc.tntech.edu/wicys/about/