REPORT

PELL CENTER for INTERNATIONAL RELATIONS and PUBLIC POLICY

SALVE REGINA UNIVERSITY

Professionalizing Cybersecurity:
A path to universal standards and status

Francesca Spidalieri and Sean Kern

August 2014

Executive Summary

The Internet, together with the information communications technology (ICT) that underpins it, has revolutionized our world and opened new opportunities for the global economy and civilization at large. Our reliance on this complex infrastructure, however, has also exposed new vulnerabilities and opened the door to a wide range of nefarious cyber activities by a spectrum of hackers, criminals, terrorists, state and non-state actors. Government agencies and private-sector companies alike have been victims of cyber thefts of sensitive information, cybercrime, and cyber disruption (e.g. denial-of-service attacks). The nation's critical infrastructure, including the electric power grid, air traffic control systems, financial systems, and communication networks, is vulnerable to cyber attacks. Compounding the problem is the reality that, as computing and communications technologies become more ubiquitous throughout society, the incentives to compromise the security of these systems will continue to rise.

The proliferating array of cyber threats has been accompanied by another realization: that there is a shortage of highly trained cybersecurity professionals who are capable of addressing the threat at hand. The dearth of advanced cybersecurity professionals can be felt across all sectors, from the federal government to the private sector, with potential negative consequences for national security, economic vitality, as well as public health and safety. As cyber threats continue to increase in scope and sophistication—and as more people become aware of these vulnerabilities—there is a growing demand for professionals who can secure our networks and combat cyber attacks. Educating, recruiting, training, and hiring these cybersecurity professionals, however, has proven to be very difficult.

This report addresses the widening gap between the supply of qualified information security professionals and the demand for skilled workers to secure critical infrastructure and cyberspace. It seeks to shed light on the current status of the cybersecurity labor market, which is best characterized as a fog of competing requirements, disjointed development programs, conflicting definitions of security roles and functions, and highly fragmented, competing, and often confusing professional certifications. It also aims to recognize the

Francesca Spidalieri is the Cyber Leadership Fellow at the Pell Center for International Relations and Public Policy at Salve Regina University.

Lt. Colonel Sean Kern, USAF, CISSP, Cyberspace Operations Officer, is currently assigned as a student at the Joint Advanced Warfighting School, Joint Forces Staff College, National Defense University. The opinions expressed here are the authors' alone and do not reflect those of the United States government or the Department of Defense.

role that education plays in developing a pipeline of cybersecurity professionals and cyber-strategic leaders ready to tackle the challenges of tomorrow.

This report offers a general overview of the cybersecurity industry with commentary from cyber experts currently working in the field. These insights will serve as points of departure for understanding specific recommendations made to guide a comprehensive cybersecurity professional development plan and create a career path that rewards and retains cyber talents in both civilian and military workforces. The report proposes an alternative to the current, ad hoc, decentralized approach to cybersecurity workforce development. Instead, this report proposes the creation of a national professional association in cybersecurity to solidify the field as a profession, to support individuals engaged in this profession, to establish professional standards and prescribe education and training, and, finally, to support the public good. The American Medical Association (AMA) and the American Bar Association provide similar functions in their respective fields.

The report's emphasis on a path forward in professionalizing the cybersecurity workforce also means that in the interest of brevity, coverage in this report cannot be comprehensive. For those interested in learning more about the existing cyber eco-system and other topics mentioned in this report, please refer to Appendices 1-4 for additional information.

Cybersecurity as a People Problem

That people, companies, and governments worldwide are increasingly dependent on information and ICT is no longer a matter of debate. With everything from our thermostats to our cars now increasingly connected to the Internet, the era of the "Internet of Things" (IoT) promises a time of near-ubiquitous connectivity and interconnection. In light of everyone's increased dependence on the Internet and ICT, cybersecurity has become one of the most critical issues facing states in the 21st century. With widespread Internet use and ever-more critical information being stored online, the specter of cyber attacks loom large. "Our adversaries in the cyber realm include spies from nation-states who seek our secrets and intellectual property; organized criminals who want to steal our identities and money; terrorists who aspire to attack our power grid, water supply, or other infrastructure; and hacktivist groups who are trying to make a political or social statement," said Richard McFeely, FBI Executive Assistant Director.[1] The security of cyberspace is now paramount, as it affects national security, economic vitality, public health and safety. It should come as no surprise, then, that Director of National Intelligence James Clapper has declared the cyber threat as the nation's foremost security concern for two years running. In addition, corporate executives and board members worldwide have ranked cyber risk as the third highest risk to their business, behind only taxation and customer loss.[2] Another area of concern is that cyber threats could have debilitating impacts on public health and safety due to the increasingly interconnectedness of systems that control the distribution of food, water, energy, and essential, life-supporting services.[3]

1. Richard A. McFeely, "FBI Statement before the Senate Appropriations Committee," Washington, DC, June 16, 2013.
2. Lloyd's, "Risk Index 2013," July 2013, http://www.lloyds.com/news-and-insight/risk-insight/lloyds-risk-index.
3. Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," Sec. 2, February 12, 2013.

Despite the growing scope and sophistication of cyber threats and the development of cyber tools as technical weapons, there are not enough people equipped with the appropriate knowledge, skills, and abilities (KSA) to protect the information infrastructure, improve resilience, and leverage information technology for strategic advantage.[4] In cybersecurity, countermeasures are implemented to reduce risks associated with the vulnerabilities of people, processes, and technology. At present, the predominant trend to combat cyber risks among organizations across all sectors is to pursue the latest security tools and technology.

While technology is certainly important to this effort, there must be an increased focus on people. No matter how good any particular technology may be, its efficacy is limited if it is not effectively adopted and implemented by management teams and correctly used by skilled employees who follow well-defined processes. Otherwise, vulnerabilities will surface that can be leveraged by both internal and external threat actors.[5] In short, any technology for combating cyber attacks is only as good as the people who develop, implement, and maintain it.

Cybersecurity issues often start with ordinary technology users who have not received proper training, do not take security seriously, or prize convenience over security by—consciously or not—sidestepping basic standards of best practices. Verizon's "2012 Data Breach Investigations Report" estimated that 97 percent of reported successful breaches could have been avoided with simple, inexpensive corrective actions.[6] Their 2014 report reaffirmed that conclusion, noting that "nearly every incident [analyzed] involved some element of human error."[7] The Ponemon Institute's 2013 "Cost of Data Breach Study" concluded that 35 percent of breaches were caused by human error and 29 percent were due to system glitches and information technology and business process failures.[8] Other post-mortems, such as the high-profile data breach of U.S. retailer Target Corp, similarly concluded that breaches would be avoidable if organizations followed commonly known cybersecurity best practices. To put it more bluntly: many successful cyber attacks—whatever their motive or intent—are enabled by operator error and lack of training. In this environment, cyber strategic leadership[9] and a team of skilled cybersecurity workers remain key to the survival of any enterprise in the digital age.

4. Francesca Spidalieri, "Joint Professional Military Education Institutions in an Age of Cyber Threat," Pell Center, August 7, 2013, http://www.salve.edu/sites/default/files/filesfield/documents/JPME_Cyber_Leaders.pdf.
5. Greg MacSweeney, "10 Financial Services Cyber Security Trends for 2013," Wall Street & Technology, December 5, 2012, http://www.wallstreetandtech.com/data-security/10-financial-services-cybersecurity-tre/240143809.
6. Verizon, "2012 Data Breach Investigations Report," http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf.
7. Verizon, "2014 Data Breach Investigations Report," http://www.verizonenterprise.com/DBIR/2014/.
8. Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis, " May 2013, https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf.
9. "Cyber-strategic leadership is […] the set of knowledge, skills, and attributes essential to future generations of leaders whose physical institutions nevertheless exist and operate in, through, and with the digital realm. These individuals need not have specific training in engineering or programming, but they must be equipped with a deep understanding of the cyber context in which they operate to harness the right tools, strategies, people, and training to respond to a dynamic and rapidly-developing array of threats." See Francesca Spidalieri, "One Leader as a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat," Pell Center, March 26, 2013, http://www.salve.edu/sites/default/files/filesfield/documents/pell_center_one_leader_time_13.pdf.

Achieving cybersecurity, in other words, is far more than a technical problem: it is fundamentally a people problem. And since cybersecurity is a people problem, there must be a human solution. In short, there needs to be a professional cybersercurity workforce, represented by a number of cybersecurity specializations, capable of inculcating standard best practices into standard professional bodies of knowledge thereby enhancing the efficiency and effectiveness of cybersecurity technologies and strategies. A comprehensive cybersecurity professional development plan, led by senior decision makers, would in turn help reduce cyber risks to our national security, economic prosperity, public health and safety.

This paper leverages the existing body of knowledge and initiatives to show the value of professionalizing the cybersecurity workforce at the level of each cybersecurity specialization, and to provide a roadmap to move forward in this effort. When discussing cybersecurity as a "profession," this report refers to the traditional definition found in the New Fontana Dictionary of Modern Thought: "a vocation that is characterized by formal qualifications based upon education, apprenticeship, and examinations, regulatory bodies with powers to admit and discipline members, and some degree of monopoly rights."

Reducing the Fog of the Cybersecurity Industry

Reports of cyber crimes, cyber espionage, data breaches, and cyber incidents surface on a daily basis. Companies are hacked, national defense technology and the industrial base are compromised, military and civilian government sites are penetrated, sensitive data is stolen, and ransomware behaves like the many-headed Hydra. While cyber threats continue to grow in both scope and sophistication, however, the cyber workforce is falling behind. The U.S. is struggling to develop and sustain the talent to protect, detect, defend, and respond to these threats.[10] The need for a knowledgeable and experienced cyber workforce has never been greater, yet its present capabilities lag behind the current threat.

In addition to the significant shortage of cyber talents, the expansion of technology innovations—such as web, mobile, cloud, social media, and IoT—are introducing new vulnerabilities and increasing companies' exploitable attack surfaces.[11] Too many organizations lack the right skills and qualified personnel to proactively assess the likelihood of a breach, to detect network infiltrations, and to mitigate attacks once they are underway. Research suggests and our interviews confirm that even organizations that can meet most of their needs internally still face difficulties in recruiting or retaining cybersecurity professionals with advanced skills.[12] The present situation, in other words, is a dangerous one.

A recently released study from Cisco Systems Inc. linked the shortage of nearly one million skilled cybersecurity professionals to growing cyber attacks.[13] In addition, a report from (ISC)^2 concluded

10. Marie Baker, "State of Cyber Workforce Development," Software Engineering Institute, August 2013.
11. Deloitte,"Transforming Cybersecurity—New approaches for an evolving threat landscape," 2014.
12. RAND Corporation, "H4CKER5 WANTED: An Examination of the Cybersecurity Labor Market," June 2014, http://www.rand.org/pubs/research_reports/RR430.html.
13. CISCO, "2014 Annual Security Report," January 2014, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

that corporate executives often lack a complete understanding of their companies' security needs and their inability to locate enough qualified security professionals, which leads to more frequent and costly data breaches.[14] These reports echo the findings of past studies, which stressed the need for a qualified cybersecurity workforce:

We not only have a shortage of the highly technically skilled people required to operate and support systems already deployed, but also an even more desperate shortage of people who can design secure systems, write safe computer codes, and create the ever more sophisticated tools needed to prevent, detect, mitigate and reconstitute from damage due to system failures and malicious acts.[15]

Although cybersecurity professionals are in great demand—and can command impressive salaries—there remains a critical shortage of people who wish to enter and thrive in this field.[16] For those who do wish to pursue cybersecurity as a career, there is a continued lack of clearly defined roles and career paths for this increasingly-vital line of work. The talent shortage in the cybersecurity labor market is exacerbated by corporate leaders who should be responsible for building a team of trusted experts, fostering a culture of security, and developing sound strategies to protect their digital investments, but instead display tendencies to treat cybersecurity as an isolated "IT problem" best left to their already overwhelmed IT departments. This approach is untenable and dangerous. As research has shown, their natural optimism bias combined with a lack of understanding of cybersecurity risks often leads business executives to believe that their company's security posture is better than it actually is, or that since they have hired the right management team, they in turn must have hired the right people to manage security risks.[17]

Managers, who do understand the need for qualified and certified cybersecurity professionals face other challenges. They do not always know how to express their security needs in realistic job descriptions, or assess the KSA of potential cybersecurity candidates. It doesn't help that no single existing certification addresses all the KSAs required for a particular position. As a result, managers often struggle to or place new cyber hires in jobs commensurate with their skill level. And businesses in general are essentially driving blind when it comes to how much, if any, investment is required to recruit, develop, and retain top cyber talents to maintain and defend their networks.

On the other hand, qualified cybersecurity practitioners do not always find the job positions advertised commensurate with the apparent demand, and cannot rely on a defined career path to assess KSA requirements for continued professional development leading to opportunities for lateral or upward movement. And students across the country, who are being told about the great job opportunities in this field, find it difficult to determine the appropriate training and education

14. Frost & Sullivan in partnership with (ISC)^2 and Booz Allen Hamilton, "The 2013 (ISC)^2 Global Information Security Workforce Study," February 2013.
15. K. Evans and F. Reeder, "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters," CSIS Commission on Cybersecurity for the 44th Presidency, Center for Strategic and International Studies, July 2010: 2.
16. A survey sponsored by Hewlett-Packard Co. and released at the 2014 RSA conference showed that about 40 percent of available cybersecurity jobs this year will go unfilled.
17. Lancope and Ponemon Institute, "Cyber Security Incident Response: Are we as prepared as we think?" January 2014.

needed to enter or advance in one of the most in-demand, profitable, and critical fields in our modern economy. On top of this, the current professional certification regime is fragmented and inadequate, and the many similar—and often competing—commercial certifications produce additional confusion for both individuals and employers. Some of these commercial certifications are even within the same specialty, such as penetration testing.

Exacerbating the overall problem is that many organizations' attitude towards cybersecurity is aloof and unconcerned—many organizations appear to reason that no matter how bad cyber threats are, they won't be a victim because they are too small, not as profitable, not part of a critical sector, already well-protected, and so forth. There are endless reasons they can give themselves to justify not adopting proper cybersecurity measures. As a result, they operate under a false sense of security, which, when compounded by the additional factors highlighted above, creates a fog in the cybersecurity industry. This fog further increases the mismatch between perception of cyber risks and reality, and between the different types of training, education, certifications, and competencies needed by the cybersecurity workforce. The end result is confusion on both the enterprise and workforce sides of cybersecurity, a situation which only benefits hackers and attackers.

To address the acute gap between market demand and supply in the cybersecurity industry—a gap that is only expected to widen as cyber jobs grow at an annual rate of 11.3 percent globally over the next five years[18]—cyber professionals (and the companies that will hire them) need a standardized way to measure their training, education, and experience in cybersecurity. They also need a well-defined career path that rewards those with higher level technical skills. As Steve Katz, the very first Chief Information Security Officer (CISO) in the industry, stated:

Information security professionals must also look at themselves as part of the entire business model, not just security, and be able to fully understand the business they are in, the problems and business risks that a certain product or service is going to address, and how to integrate security into business, and business into security. Their soft skills should include being able to communicate, negotiate, and develop relationships within the C-suite, so that they can be present when privacy or a corporate strategy is being discussed.[19]

On the other hand, modern boards of directors and C-suites must view cyber risk as a component of their overall enterprise risk management process rather than a compliance issue, and take ownership of their company's cybersecurity. Companies must integrate cybersecurity front and center into their daily activities and must anchor it into their decision-making processes in a holistic and comprehensive manner. No company or agency can ignore cybersecurity; it is the source of systemic risk and potential damaging "material effects" that can hurt an organization's profits, value, brand, and financial future.[20] In an effort to combat these potential downsides, employers need a standard approach by which they can evaluate cyber workers' skills and

18. Frost & Sullivan, 2013.
19. Author's interview with Steve Katz, President of Security Risk Solutions LLC and Executive Advisor at Deloitte, July 7, 2014.
20. James Lewis, "Raising the Bar for Cybersecurity," Center for Strategic and International Studies, February 12, 2013.

competencies quickly and accurately in order to harness the right people to the right challenges in a rapidly-evolving environment.

The Role of Education

Over 300,000 cybersecurity jobs are estimated to be vacant just in the United States today. Among those, 83 percent require a bachelor's degree or higher.[21] From the federal government to the Fortune 500, the demand for educated and experienced cybersecurity professionals is only expected to increase in upcoming years, especially as organizations face data breaches and cybersecurity threats with unprecedented frequency. Yet there remains a noticeable mismatch between this burgeoning demand for cybersecurity talents and the efforts underway to "develop professionals who can build and manage secure, reliable digital infrastructures and effectively identify, mitigate, and plan for asymmetric and blended threats."[22] Although only one of the components—and not a sufficient one alone—in the creation of a sound cybersecurity workforce, education must be the first step in developing a cadre of cybersecurity professionals and cyber-strategic leaders who are prepared to meet tomorrow's challenges today.

The U.S. government addressed the education of a cyber workforce as part of its 2008 Comprehensive National Cybersecurity Initiative (CNCI), which included a number of mutually reinforcing initiatives designed to secure the United States in cyberspace. Its eighth (unclassified) initiative out of 12 called to:

> **Expand cyber education.** While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950's, to meet this challenge.[23]

Many of today's activities, including the establishment of the National Initiative for Cybersecurity Education (NICE) and other government-founded efforts aimed at moving more cybersecurity graduates through the pipeline, date back to the CNCI and the money allocated in support of

21. The Abell Foundation & CyberPoint International LLC, "Cybersecurity Jobs Report," January 8, 2013: 19, http://www.ctic-baltimore.com/reports/Cyber%20Security%20Jobs%20Report-010813.pdf.
22. Michael Assante and David Tobey, "Enhancing the Cybersecurity Workforce," *IT Professional*, vol. 13, no. 1, 2011: 12-15.
23. White House, "The Comprehensive National Cybersecurity Initiative," January 2008, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative. Emphasis in original.

this initiative.[24] However, despite the large increase in cyber education since the release of the CNCI and the growing number of college and university programs teaching computer science, programming, and information technology, this highly specialized but ill-defined workforce still suffers from underinvested educational pipelines and disjointed development programs.

When it comes to scaling the education pipeline to meet the challenges facing the modern workplace, then, a lot remains to be done to fill the education gap. The National Science Foundation (NSF) and the National Security Agency (NSA), among others, have started to address this issue. The NSF and the Department of Education, for example, are leading the Formal Cybersecurity Education component of NICE, aimed at bolstering cybersecurity education programs encompassing kindergarten through twelfth grade, higher education and vocational programs.[25] The NSA and Department of Homeland Security (DHS), on the other hand, have jointly sponsored the National Centers of Academic Excellence in Information Assurance (IA) Education (CAE/IAE), Research (CAR-R), and CAE Cyber Operations.[26] These programs are deeply technical and centered around information assurance—limited to the protection and management of information-related risk—and rarely pursue broader multi-disciplinary approaches commensurate with the complexity of cybersecurity.[27] Moreover, even if the centers-of-excellence designation had the potential to represent an educational baseline, only 186 institutions have received the CAE accreditation—which is less than 5 percent of all American colleges and universities. And although cybersecurity is not inherently a governmental concern, the only existing cybersecurity-related education accreditation program to date is government sponsored. This is a flawed approach.

As Melissa Hathaway, who led the development of the CNCI and then President Obama's Cybersecurity Policy Review, stated:

> The problem is that we are not even teaching the basics of computer security in schools and university programs in general, and that cybersecurity is still not part of most computer science departments and other university departments' core curricula... We will never get to the workforce needed until we have the majority of schools and universities teaching the basic skill sets required in the field and this becomes part of a standardized core curriculum, just like basic history, math, and other basic courses. Cybersecurity, after all, is part of everyday life![28]

It must also be recognized that "cybersecurity is a complex subject whose understanding requires

24. RAND Corporation, "H4CKER5 WANTED," 2014.
25. National Initiative for Cybersecurity Education, "NICE Component 2: Formal Cybersecurity Education," http://csrc.nist.gov/nice/education.htm.
26. NSA/DHS Centers of Academic Excellence Institutions, http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.
27. Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority," *Joint Forces Quarterly* 68, no.1, January 2013: 53-58.
28. Author's interview with Melissa Hathaway, President of Hathaway Global Strategies LLC and Senior Advisor at Harvard Kennedy School's Belfer Center, June 20, 2014.

knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law."[29] Although technical measures are an important element of cybersecurity, we cannot expect new technologies alone to protect an organization's information and business, nor we can expect cybersecurity professionals to be the only ones in charge of preventing and containing cyber threats. As discussed in the sections above, skilled workers, as well as institutional and business leaders, must have a deep understanding of cybersecurity. These individuals need not have specific training in engineering or programming, but they must be equipped with knowledge of the cyber context in which they operate to harness the right tools, people, strategies, and solutions to achieve competitive advantage.

Despite the pressing need to educate future generations about cybersecurity, few American universities and colleges offer courses or degree programs that combine cybersecurity technology, policy, business and other disciplines, and even fewer encourage collaboration among departments to optimize their efforts and insights available from cross-fertilization.[30] Current cybersecurity programs should be expanded and incorporated into all major non-technical university programs and technical professional development programs, from community colleges and technical institutes to graduate and doctoral degree programs, as well as professional certification programs (e.g. the Certified Information Systems Security Professional (CISSP)). In addition, these programs will need a comprehensive framework to integrate common best practices, core curriculum tenets, and minimum standard requirements.

There is an obvious mechanism for the federal government to impose minimum cybersecurity curricular standards. The Department of Education could provide "financial assistance to individuals, schools, states and their subdivisions to assure that trained manpower of sufficient quality and quantity meet the national standard of the U.S."[31] This, in fact, was the intention of the 1958 National Defense Education Act (NDEA), signed into law at a time of growing concern that U.S. scientists were falling behind scientists in the Soviet Union. It aimed at strengthening the national defense and encouraging and assisting in the expansion and improvement of educational programs to meet critical national needs.[32] This federal policy helped establish minimum educational standards, particularly in math and science, and authorized both National Defense Fellowships and loans for collegiate education and state educational agencies. A national investment in cybersecurity education programs—perhaps in the form of matching funds—would effectively establish minimum curriculum standards for cybersecurity. If it could be done for the Cold War, it can be done for the age of Cyber War.

The challenges inherent in creating a federally-dictated, top-down set of standards for cybersecurity education and training are not modest. But even if they were easily overcome, they would not be

29. National Research Council, "At The Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues," Washington, DC: The National Academies Press, 2014.
30. Spidalieri, "One Leader at a Time," 2013.
31. Melissa Hathaway, author's interview, 2014.
32. *United States Statutes at Large*, vol. 72, 85th Congress, 2nd Session, 1958: 1580-1605.

sufficient to the challenge at hand. Professionalization of the cybersecurity industry, as this report argues, requires a nationally recognized, independent professional association, whose responsibility would also include establishing standardized core curricula in information technology and cybersecurity for educational institutions at all levels, and encouraging intra-university collaboration (more in subsequent sections).

The blistering pace of technological change and the cyber threats that accompany it are only going to accelerate, and the lack of a well-educated security workforce poses dire consequences for our collective future. If the mismatch between our cyber defense capabilities and skilled professionals remains on its current trajectory, cyber threats will have the potential to undo much of the economic, social, and military gains that cyberspace has enabled. Educational institutions and organizations of all sizes and sectors have a tremendous opportunity to turn this challenge into an opportunity. Cybersecurity can make good business sense and those organizations embracing cyber opportunities stand to gain significant advantage in an increasingly competitive global marketplace. The missing piece to navigate the fog of the cybersecurity industry, however, is to create an overarching organizational framework to develop, manage, and oversee the training, education, certification, and continuous professional development of a qualified cybersecurity workforce along a career continuum, and to guide leaders across society in placing the right people with the right knowledge, skills, and abilities in the right position to create a safer, more secure cyberspace for everyone.

A Proactive Approach to Cybersecurity Workforce Professionalization

Evans and Reeder expressed the challenge elegantly:

> In many ways, cybersecurity is similar to 19th century medicine—a growing field dealing with real threats with lots of self-taught practitioners only some of whom know what they are doing. The evolution of the practice of medicine mandated different skills and specialties coupled with qualifications and assessments. In medicine, we now have accreditation standards and professional certifications by specialty. We can afford nothing less in the world of cyberspace.[33]

Numerous studies have pointed out the necessity to grow and retain a pool of highly skilled cyber professionals. Reports by the Center for Strategic and International Studies,[34] the Department of Homeland Security's Homeland Security Advisory Council,[35] RAND Corporation,[36] and Booz Allen Hamilton[37]—just to name a few—have outlined the difficulty of meeting cybersecurity manpower needs, especially in the federal government, and offered a series of recommendations to manage the

33. Evans and Reeder, 3.
34. Ibid.
35. U.S. Department of Homeland Security's Homeland Security Advisory Council, "CyberSkills Task Force Report," Fall 2012.
36. RAND Corporation, "H4CKER5 WANTED," 2014.
37. Partnership for Public Service and Booz Allen Hamilton, "Cyber IN-Security: Strengthening the Federal Cybersecurity Workforce," Partnership for Public Service, July 22, 2009.

supply-demand balance for cybersecurity workers. The problem, however, is that while the critical shortage of skilled cybersecurity professionals has been widely recognized and several initiatives attempting to address the issues of cyber workforce development have been advanced, none of these efforts have yielded comprehensive results. Indeed, there has been no significant attempt to create a unifying strategy to prioritize existing and planned cybersecurity initiatives. Neither have efforts succeeded in establishing accreditation standards for cybersecurity curricula and certifications nor elevating and standardizing the competencies of the cyber workforce. In addition, efforts have failed to address the lack of an overall, integrated approach to fill the lower and middle-void of adequately skilled workers, let alone address professionalization of the cybersecurity industry.

As James Lewis, Director of the CSIS Strategic Technologies Program, explains, "Professionalization would be the mastery of certain skill sets essential for success, some way to demonstrate that you have acquired those skills, and then that you can refresh that knowledge through continuing education. If you think about professionals in any field," he continued, "they need to have the right skills and competencies, and they have to be able to show that they posses them." Thus, in order to professionalize the cybersecurity industry, "you have to first identify the body of knowledge and skills that professionals need to have to work effectively in this field; then find a way to provide those skills through education and training programs; and finally have a way to accredit this process (both those identifying the body of knowledge and those teaching it) and attest that the individual has acquired those skills.[38]

One of the strongest arguments against professionalization, however, is that cybersecurity is still too new a field in which to introduce professionalization standards for its practitioners and that it is changing too rapidly to impose standards now—which some argue that would risk imposing rigidity on a growing and changing field. This was the conclusion reached by the National Research Council (NRC) in 2013 and detailed in their report "Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-making." The report offered three main reasons to oppose professionalization. First, they argued that the knowledge, skills, and abilities required of the cybersecurity workforce are so dynamic that one cannot effectively establish a baseline for professionalization. Second, complementary to the first, the report asserted the knowledge and competencies required by the cybersecurity workforce are too broad and diverse to enable professionalization. Finally, they noted that in a time where demand for cybersecurity workers far exceeds supply, professionalization would create additional barriers to entry.[39]

The evidence in the cyber realm and the historical similarities with the professionalization of other important fields in our society, however, undercut the strength of the NRC's argument. First, the cybersecurity workforce should not be treated as a homogenous population. NICE is the recognized authoritative source in this area and has defined the cybersecurity workforce in a consistent way using a standardized lexicon, but has not suggested that it should be referred to as a singular,

38. Author's interview with James Lewis, Director and Senior Fellow of the CSIS Strategic Technologies Program, June 19, 2014.
39. National Research Council, "Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-making," Washington, DC: The National Academies Press, 2013.

unique occupation. The NICE National Cybersecurity Workforce Framework 2.0 (NCWF) used an organizational construct to group similar types of cybersecurity work around seven broad categories or areas of practice:[40]

- Securely Provision;
- Operate and Maintain;
- Protect and Defend;
- Investigate;
- Collect and Operate;
- Analyze; and
- Oversight and Development.

Within each of these areas, specific job functions are described along with sample job titles, totaling 31 different specialty areas characterized by particular tasks, knowledge, skills, and abilities (Appendix 1). Obviously, not all specialties are created equal in terms of criticality and job requirements, and they exhibit varying levels of maturity. As Tony Sager, Director of the SANS Innovation Center, explains

> The time seems ripe at least for the professionalization of some of the more mature specialty areas, where there is already a broad body of knowledge, common training, certifying institutions, and somehow well-defined jobs… Some of the areas prime for professionalization could be penetration testing, red teaming, and forensics analysis.[41]

For those specialties that may not be quite as ready for formal professionalization, they would still greatly benefit from having a unifying framework of reference and a national member association that would accelerate the rate of professionalization for its specialty. The American Medical Association (AMA), for example, was founded in 1847 to address the very same issue—the lack of professionalization in the medical field.[42] During the early nineteenth century, the major concern was that the medical profession was increasingly over-run with self-taught practitioners—only some of whom knew what they were doing. The tide started to turn when it was decided that the risk to the public was simply too great to bear, and a movement began to minimize "self-taught practitioners" and professionalize the industry.

The AMA accelerated the professionalization of medicine and the establishment of minimum standards in medical training, education and apprenticeship requirements to gain entry to the profession. The same should be done in the cybersecurity field with a similar cybersecurity national body and professional associations. Like the medical profession of the nineteenth century, the present cybersecurity industry features too many "self-taught practitioners" who have varying

40. National Initiative for Cybersecurity Education (NICE), "National Cybersecurity Workforce Framework, version 2.0," May 2014, http://niccs.us-cert.gov/training/tc/framework/categories.
41. Author's interview with Tony Sager, Director of the SANS Innovation Center, June 5, 2014.
42. NICE, "A Historical Review of How Occupations Become Professions," Version 1.0, 2012, http://csrc.nist.gov/nice/documents/a_historical_view_of_how_occupations_become_professions_100312_draft_nice_branded.pdf.

degrees of knowledge and training. Unlike the medical field of the 1840's, the cybersecurity field is increasingly chaotic and fragmented. This will continue without a unifying strategy for professionalization.

Secondly, specific cybersecurity competencies and a baseline of capabilities can actually be identified and categorized, while additional KSAs can always be developed and added as technology advances and new risks emerge. In fact, as another report from the National Research Council recognizes:

> The specifics of cybersecurity change rapidly, but the fundamental concepts and principles endure, or at least they change much more slowly. These concepts and principles are approximately independent of particular cybersecurity technologies or incidents, although they manifest themselves in a wide variety of different technologies and incidents.[43]

Ongoing professional education is required in any critical profession, such as medical doctors, where there exists a rapidly changing body of knowledge. This will be a necessary requirement in the cybersecurity field as well, because although the specific instances of new attacks may change quickly, the mechanisms to manage them will have some permanence and basic security concepts and principles will persist, while additional KSAs will be developed over time. Some commercial certification organizations already account for this, requiring members to accrue various levels of continuing professional education annually.[44] Moreover, in comparison to the 24 general certificates and 125 subspecialty certificates listed by the American Board of Medical Specialties, the seven categories and 31 specialty areas identified by NICE show that the breadth and depth of cybersecurity specialties is certainly comparable to that of the medical professions.

As for the argument that the nation's cybersecurity workforce is too broad and diverse to be treated as a single profession, this again can be compared to the medical field, where there is a large array of specialties—surgery, psychiatry, family care, etc.—in which individuals can pursue careers. Cybersecurity jobs have a similar degree of variation: one can be a network administrator responsible for analysis, installation, and configuration of a small company's network, or a security engineer in charge of protecting a major nuclear plant from cyber threats and exposure. As NICE explains in its report "A Historical Review of How Occupations Become Professions," each job category of the medical field, like in cybersecurity, can be broken down further into specialty areas, each with "a unique role and set of knowledge and skills that are required to perform this role. As with most fields, some responsibilities, knowledge, and skills might be the same for multiple roles."[45] For example, while in smaller organizations with fewer staff, cybersecurity job positions may require competence across different specialty areas, larger organizations with very large staffing abilities, may be able to assemble a team of cybersecurity professionals, with each member being a skilled practitioner in one primary specialty.

43. National Research Council, "At The Nexus of Cybersecurity and Public Policy," 2014.
44. (ISC)², "Maintaining Your Credential," https://www.isc2.org/maintaining-your-credential.aspx.
45. NICE, "A Historical Review of How Occupations Become Professions," 2012.

The problem, however, remains the astounding breadth of concerns in the cyber realm, the lack of a clear definition of security roles among application designers, developers, quality assurance teams, and operations teams, and the lack of specific job-role task details that continue to fragment the industry and cause additional confusion. Even the existing training frameworks—such as those developed by NICE, USCYBERCOM, and the Defense Information Systems Agency—which use very similar wording for job roles and functions, do not provide details on the specific tasks performed as part of those job roles.[46] Professionalization would help in clarifying the particular duties regularly performed while in a specific job role, the skill level required to be effective at those duties, and the specific professional standards and requirements necessary for the position, regardless of the sector or organizational structure in which the cybersecurity professional is employed.

By identifying the knowledge, ability, and skills necessary to operate competently within a functional role, the varying levels of formal education, licensure, work experience, and knowledge requirements could be similarly identified. Defining roles and knowledge requirements, for instance, helps medical workers in various specialties gain recognition and acceptance, and it helps ensure that medical workers meet sufficient and consistent knowledge requirements. In addition, professionalization has the potential to attract workers, orient the workforce to more effectively consider future factors that may affect the evolution of the profession, and establish a long-term path to enhancing quality of the workforce with a standardized set of specific KSAs.

Finally, the NRC report argues that professionalization would impose additional barriers to entry in the cybersecurity industry and inadvertently screen out suitable candidates. Professionalization does indeed create some barriers to entry, but this is not so much a powerful criticism as the whole point of professionalization. By definition, more rigorous curriculum standards, higher training, and more stringent certification requirements will create some barriers to entry. Higher barriers to entry, indeed, can yield some desired benefits: they are intended to reduce the risks that unqualified workers pose to organizations once positioned to serve in a specific role. Just like in the medical field, some cybersecurity positions pose greater risks to security, public health and safety, and economic viability than others. For example, the insider threat posed by an unqualified or disgruntled employee with trusted access to sensitive systems and information—think of Edward Snowden—could cause incredible damage. Not all cybersecurity positions are created equal in terms of job requirements and risk posed to organizations and therefore the risk may well be worth a diminished supply due to the barriers imposed by professionalization.[47] The rigor of professionalization may also discourage those who are not dedicated to professional ethical standards, just like being subject to a polygraph examination may deter potential candidates with something to hide. Ultimately, the process of professionalization involves acculturation with

46. For a detailed analysis of DoD and Federal civilian agencies' training and development initiatives, see Baker, "State of the Cyber Workforce Development," 2013.
47. Jane Lute, Deirdre Durrance, and Maurice Uenuma, "Mission Critical Cybersecurity Functions," Council on Cyber Security, February 2014, http://www.counciloncybersecurity.org/workforce/cybersecurity-roles/.

respect to core values and ethical standards, which would ensure that the critical mission, business information, and infrastructure cyber workers are entrusted with, are privileged and protected.

The NRC report's main conclusion is that attempts to professionalize a cybersecurity occupation should only be undertaken when the field is "well-defined" with "stable knowledge and skill requirements," and that there is credible evidence of skill deficiencies in the workforce. This is a fair statement and any workforce development strategy must first consider the challenges inherent in this highly dynamic field. Simply certifying expertise grounded in outdated methods and tools could become a liability rather than an asset. It is also important to recognize that the field will remain dynamic, as it is the reflection of the constant innovation and creativity spurred on by rapid decreases in the time and effort to deploy technology in scale.

As Jane Holl Lute, former deputy secretary of the Department of Homeland Security and current president of the Council on CyberSecurity, and Michael Assante, a member of the Council's board of directors and a former president of the National Board of Information Security Examiners, eloquently argued:

> We can no longer live in a cyber world without performance expectations for those who design, operate, and maintain our systems and our networks… The many women and men we know in the civilian cyber workforce want to be held to higher standards, they want to demonstrate their ability to practice their trade with skill and precision, and they want clear acknowledgment of their proficiency. Using acknowledged processes and standards of best practice and professionalism to ensure that these individuals are competent, prepared and capable of making correct decisions day-to-day and during an emergency will be critical to the success of any effort to improve the security of information networks.[48]

Currently, there are a number of independent initiatives in both the public and private sectors to address specific aspects of cybersecurity workforce development, but there is no unifying strategy connecting them all. As a result, the longer the cybersecurity workforce waits to professionalize, the more unwieldy this environment will become, which will make it increasingly difficult to unify all stakeholders under a common strategy in the future. As the old adage goes, that which is not measured is not managed. A cybersecurity workforce professionalization strategy can serve as a framework to measure progress. Nature also shows us that systems tend to disorder unless properly managed. But "professionalization will require an organized effort; we cannot wait for the field to figure itself out," explained Michael Assante.[49] Our country's increasing reliance on secure,

48. Jane Holl Lute and Michael Assante, "Higher Ground: Why We Must Begin Professionalizing the Nation's Cybersecurity Workforce Now," *Inside Cybersecurity*, October 11, 2013, http://insidecybersecurity.com/Cyber-General/Cyber-Public-Content/higher-ground-why-we-must-begin-professionalizing-the-nations-cybersecurity-workforce-now/menu-id-1089.html.

49. Author's Interview with Michael Assante, SANS project lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security, June 5, 2014.

reliable, and safe cyber systems cannot afford to "wait for some 'natural' progression in the pursuit of clear competency and performance standards for cyber professionals," Mr. Assante continued. And in the background of all this looms a grim reality: as we wait for cybersecurity workforce professionalization, cyber threats and cyber attacks will only grow.

As Dr. Ernest McDuffie, Lead for the NICE initiative, reminded us "there is no unifying strategy or single organization that could take ownership of the field at the moment." In other words, there is no focal point or center of gravity around which to organize. "There are a lot of organizations with great expertise," Dr. McDuffie continued, "but no central organization with the credibility and capability to serve this role. The only organization with the credibility [to lead the professionalization of this field] would be a hybrid between academia and business, with an international presence and recognized track record."[50]

This report, however, argues that an effective alternative to today's ad hoc, decentralized approach to enhancing cybersecurity, will require the development of a comprehensive framework for professionalization and the establishment of a national, independent, non-profit organization to serve as a representative body and clearinghouse for the cybersecurity profession. We recognize that the professionalization process would unfold over the course of several years and would involve stakeholders from government, academic institutions, profit and non-profit organizations, public and private sector entities, formal and informal groups. This process would leverage existing organizations while also require the development of new ones as well.

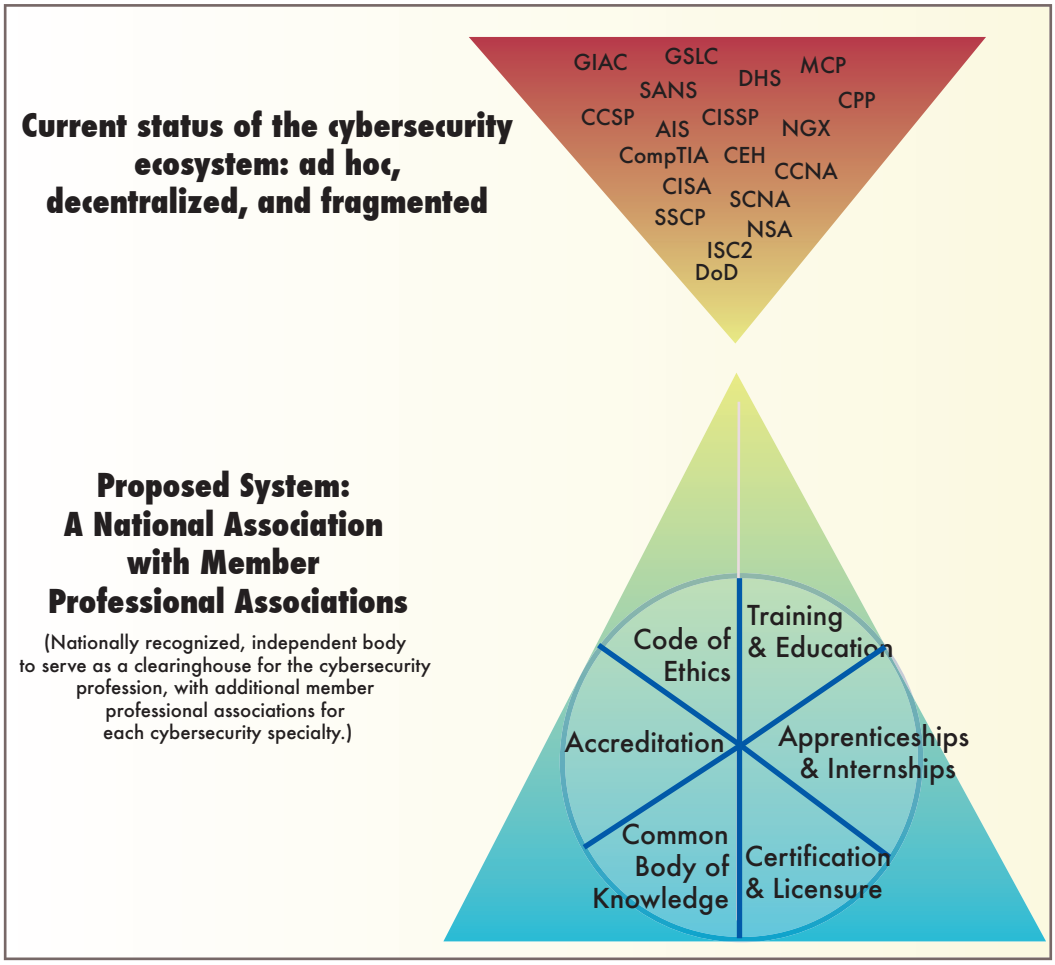
Our hope is that this work catalyzes additional research and efforts to unify this complex ecosystem under a common purpose, seek ways to mobilize commitment to change, develop a shared vision, foster consensus, and institutionalize a commonly accepted approach. The actions or strategic objectives proposed in the next section are intended to help professionalize the cybersecurity workforce following the traditional model of professionalization as represented by the medical profession:

- Create a nationally recognized, regulatory body to serve as a clearinghouse for the cybersecurity profession, similar to AMA in the medical field;
- Establish member professional associations for each specialty;
- Develop a common body of knowledge (CBK) for each specialty;
- Establish and maintain rigorous standards of training and education;
- Establish certification/licensing requirements;
- Establish apprenticeship, residency requirements for each specialty; and
- Establish a standard code of ethics.

Recommended Action Plan

The following are recommended strategic objectives to guide a national, comprehensive effort to professionalize the cybersecurity workforce. The seven strategic objectives presented below are derived from the traditional model of professionalization adopted by the medical field. Note that

50. Author's interview with Dr. Ernest McDuffie, Lead for the federal National Initiative for Cybersecurity Education (NICE), June 2, 2014.



any reference to "cybersecurity specialty" is in the context of the specialties defined in the NICE Cybersecurity Workforce Framework (See appendix 1).

Recognizing that cybersecurity is a complex socio-technical-economic ecosystem, populated by many different stakeholders relevant to its professionalization, a comprehensive strategy will necessarily include academic institutions, for-profit and non-profit organizations, public and private sector entities, formal and informal groups, and recognized cyber-strategic leaders in the field.

Strategic Objective 1:
Create an Independent, Nationally Recognized Cybersecurity Professional Body.
The best way to move forward in a comprehensive manner is to first and foremost leverage existing efforts and initiatives to advance cybersecurity workforce professionalization. Given the complexity of the current cybersecurity eco-system, however, there is no single organization in existence today that has the credibility and capability to serve as a national professional body. An alliance or consortium of existing professional associations could serve as the starting point to create a national, independent governance body, similar to other private and public collaborative models in practice. This organization would serve as a national representative of the cybersecurity

profession as a whole, much like the AMA. Through education, development of core curriculum standards, licensure advocacy, leadership training, multi-disciplinary networking, and outreach, this body would enhance the image of its members and their ability to ethically and professionally practice the cybersecurity profession. A national independent body would also be responsible, or at least initially help the federal government, establish minimum core curriculum standards and requirements in information technology and cybersecurity for educational institutions at all levels.

A more mature national organization would include representatives of the following (some of whom may overlap):

- Major private sector organizations that employ cybersecurity professionals;
- Cybersecurity-related member associations;
- Cybersecurity-related certifying bodies;
- Universities with major cyber education and research programs; and
- Key federal government agencies.

Appendix 2 provides a sample of existing professional computing organizations compiled by the NIST Computing Resource Center that would be considered important stakeholders in this body. To this group, we would also include the Council on Cyber Security, the Institute of Electronic and Electrical Engineers (IEEE), and the Association of Computing Machinery.

Ultimately, this body would serve as a clearinghouse for the cybersecurity profession and a focal point for education, training, communication, participation, facilitation, support, and negotiation within the cybersecurity workforce.

Although the creation of an initial alliance or consortium of existing professional associations is certainly conceivable, no such entity has emerged yet. As Michael Assante noted "security is so diverse and shared that organizing around it conflicts with any known organizational principle… Most organizations think, 'If we tried to professionalize the workforce, we would probably fail so it is not worth our investment.'"[51]

An alternative organizational construct could be a Federally Funded Research and Development Center (FFRDC). For instance, the Department of Defense's Software Engineering Institute (SEI) provides an excellent example of this model. SEI revolutionized the development of complex software systems through the development of the Capability Maturity Model-Integrated (CMMI). The CMMI became the basis of DoD's software procurement contracts and, as a result, the industry standard in the private sector too. The CMMI has now spun off into a separate, entirely independent organization. Currently, NIST is reviewing proposals for a first Cybersecurity FFRDC to be managed by the National Cybersecurity Center of Excellence (NCCOE). This FFRDC's mandate, however, would be solely technology-driven. A complementary cybersecurity workforce mandate, that would follow the recommended strategic objectives exemplified in this report, could see the same success achieved by SEI. Tony Sager expressed his support for a FFRDC approach as a

51. Michael Assante, author's interview, 2014.

"clever model" that would ameliorate his and others' concerns of leaving professionalization merely to "commercial interests."[52]

Strategic Objective 2:
Establish Cybersecurity Specialty Professional Associations.
The national body cannot and should not determine the specific professionalization requirements for each cybersecurity specialty. This role should belong to the senior practitioners of a given cybersecurity specialty who would serve as governing members of the specialty association. The national body would then provide oversight and assistance to establish professional associations for each specialty, which will serve as member associations of the national body. This model is similar to the AMA, which includes professional associations for each medical specialty (e.g., American Academy of Physician Assistants).

There are currently no representative professional associations for the 31 NCWF specialties. Once established, each professional specialty association would serve as principals, along with the national body, in implementing the remaining strategic objectives.

Strategic Objective 3:
Develop and Maintain a Professional Common Body of Knowledge (CBK).
Each specialty professional association will be responsible for developing and maintaining its specialty's professional body of knowledge. Initially, the NIST National Cybersecurity Workforce Framework's specialty knowledge, skills, and abilities, and DHS/NSA's Centers for Academic Excellence criteria could be used as a basis for each specialty's body of knowledge. Other sources may come from existing CBKs defined by organizations that offer relevant professional certifications for the given specialty. One example would be the body of knowledge developed by the International Information Systems Security Certification Consortium (ISC)[2] Certified Information Systems Security Professional (CISSP), which is applicable to the specialties included in the "Oversight and Development" category. This issue is addressed in more detail below.

Strategic Objective 4:
Establish and Maintain Required Levels of Training and Education.
A profession typically requires rigorous, extensive training and education. Training is typically task-centered, while education is related to developing comprehensive knowledge of a subject. Not all specialties will have the same levels of training and education much like the medical profession's Certified Nursing Assistants, Licensed Practical Nurses, Registered Nurses, Physician's Assistants, Physicians, and Hospital Administrators. Each have varying levels of training and education commensurate with the body of knowledge and skills needed for specific core functions in order to reduce the risk of a practitioner failing a patient, their organization, or the public at large.

An essential element of the education process is ensuring that the programs supporting the different specialties are accredited in a similar fashion to the NSA/DHS National Centers of

52. Tony Sager, author's interview, 2014.

Academic Excellence in IA's accreditation standards. Since this field is not inherently governmental and information assurance is only one component of cybersecurity, it is reasonable to envision a future in which the NSA and DHS may serve as advisory board members to the national body and relevant specialty associations in order to ensure their cybersecurity workforce needs are met, but would no longer maintain an accreditation program in-house. Instead, the cybersecurity community would leverage an existing accreditation body, such as the Accreditation Board for Engineering and Technology (ABET), for cybersecurity education accreditation.

ABET currently accredits 3100 science, technology, engineering, and management (STEM) programs at 670 institutions in 24 countries. It has two accreditation commissions that would suit the requirements of the cybersecurity profession, the Computing Accreditation Commission and the Engineering Accreditation Commission. Additionally, ABET has member associations affiliated with areas related to cybersecurity. Each of ABET's members has responsibility for an academic discipline within applied science, computing, engineering, or engineering technology at the postsecondary level. Appendix 4 provides additional detail regarding ABET's structure and the cybersecurity-related degree programs it currently accredits.

Urgency is needed in this area as a number of cyber-related undergraduate and graduate programs are being developed across the United States and abroad.[53] Without formal accreditation guidelines, it will be difficult to assess the efficacy of those programs. Defining ways to accredit and measure education and training is an essential task under this objective.

Strategic Objective 5:
Establish Certification/Licensing Requirements.
Professions typically have some regulatory body responsible for establishing certification and/or licensing requirements before a candidate can actually serve in a professional capacity. Some professions have state or even national level licensing requirements. For example, a physician is required to take a state exam in each state he or she wishes to practice. The specialty professional associations we speak of in this report would need to determine if this model or the current commercial models make the most sense.

The main issue is that most of the professional cybersecurity certifications currently available are "focused on demonstrating expertise in documenting compliance with policy and statutes rather than expertise in actually reducing risk through identification, prevention, and intervention."[54] Compounding the problem is "the chaos of the certification process and the many home-brewed, self-declared certifications, with all their competing ideas," stated Tony Sager.[55] "We do not even have a way to compare all the different certifications, and the certifying companies do not really have an interest in collaborating," Mr. Sager continued.

53. Sean Kern et al., "Senior Cyber Leadership: Why a Technically Cybersecurity Workforce is Not Enough," Cyber Security Forum Initiative, http://www.csfi.us/pubdocs/?id=39.
54. Evans and Reeder, 8.
55. Tony Sager, author's interview, 2014.

Bringing the existing multiple, competing, mostly profit-driven certifying organizations, that offer different certifications for many of the cybersecurity specialties, under a common umbrella may prove the most challenging task in this strategy. This also begs two fundamental questions. First, who certifies the certifier? Second, how should employers assess multiple, competing certifications when reviewing potential candidates?

Cybersecurity practitioners, hiring authorities, and customers would be better served by a single specialty certification. Unfortunately, current certifications do not map directly to defined cybersecurity specialties. For example, a number of different cybersecurity specialties require some level of knowledge of penetration testing. These same specialties require knowledge in other areas that are covered by yet other certifications. It would make more sense to certify a professional in a given specialty than requiring him to hold multiple certifications in order to prove his knowledge for a required specialty.

Each professional specialty association should develop its own certification regime, which would include a tough educational component and a monitored practical component. This would eliminate the need for an employee to maintain multiple certifications. The professional specialty association would work with existing related commercial certifying organizations to develop a best of breed certification regime based on each specialty's CBK. Existing commercial certifying organizations would still play a critical role in the cybersecurity workforce development, but their roles and responsibilities would shift. Rather than owning the intellectual property of their organically developed CBKs, certifying organizations would contribute to the CBK maintained by a given specialty association. Certifying organizations would still provide training and certification administration, just as they do now. This is somewhat similar to SANS' recent decision to transition its "20 Critical Security Controls" intellectual property to the Council on Cyber Security. It would require a degree of altruism and honest acknowledgment of the benefits of the proposed regime on the part of the certifying organizations, but the existing business model would still hold.

Appendix 3 lists a number of current certifying bodies compiled by the NIST Computing Resource Center as well as the joint NICE and Federal CIO Council's 2012 "IT Workforce Assessment for Cybersecurity" report.

Strategic Objective 6:
Establish Apprenticeship, Residency Requirements.
Professions are traditionally organized into various tiers based on experience, such as apprentice, journeyman, and master. These tiers, in addition to being differentiated by education, training, and certification requirements, are also differentiated by apprenticeship and/or residency requirements. In practice, the junior professional is placed under the direct supervision of a seasoned, professional for a predetermined period of time. This provides a controlled environment in which the junior professional can practice the knowledge and skills gained through previous training, education, and experience. Some cybersecurity specialties may not require apprenticeship or residencies. Each specialty association would judge their need for this component.

Strategic Objective 7:
Establish a Standard Code of Ethics.
Most certification organizations currently have a code of ethics. For example, (ISC)[2] has a code of ethics consisting of four canons:

- Protect society, the common good, necessary public trust and confidence, and the infrastructure;
- Act honorably, honestly, justly, responsibly, and legally;
- Provide diligent and competent service to principals; and
- Advance and protect the profession.[56]

The Information Systems Security Association (ISSA) also has a code of ethics. There would be little to no conflict in developing a standard code of ethics for the national body and special member associations. The core values and ethical standards developed in each association would in turn ensure that the critical mission, business information, and infrastructure that specific cyber workers are entrusted with, are privileged and protected.

Conclusion

Our cybersecurity issues and needs are complex and widespread, but a comprehensive cybersecurity professional development plan and career path to reward and retain cyber talents have yet to emerge. Given the importance of cyber to our national security and standard of living, we need a professional workforce with common KSAs within a professional framework and a number of specializations, just as the medical, legal, and other critical professions do. There must be consistency of expectation of the specific cyber KSAs that the workforce obtains from any given educational delivery method and source. To do this as effectively and transparently as possible in this global environment, the cyber community must professionalize their craft.

This report proposed an alternative to the ad hoc, decentralized approach to enhancing cybersecurity that marks today's cybersecurity profession. The establishment of a nationally recognized, professional association to serve as a clearinghouse for the cybersecurity profession (similar to AMA in the medical field), and of additional member professional associations for each identified specialty within the cybersecurity industry, would help reduce the risk currently posed by a wide variety of cyber threats. Although an alliance or consortium of existing professional associations could serve as the starting point for this body, a department or agency sponsored FFRDC (similar to the DoD's Software Engineering Institute) would be better suited to serve as the organizing construct for this new entity. Indeed, an FFRDC with the mandate to plan, direct, and oversee the implementation of the strategic objectives outlined in this report could mitigate and potentially eliminate the current fog of competing requirements, disjointed development programs, conflicting definitions of security roles and functions, and highly fragmented and inadequate professional certifications, resulting in reduced risk and increased competitive advantage for all.

56. (ISC)[2], "Code of Ethics," https://www.isc2.org/ethics/default.aspx.

Appendix 1: NICE Cyber Security Workforce Framework Categories and Specialties[57]

Category	Specialties
Securely Provision	Information Assurance Compliance Software Assurance and Security Engineering Systems Security Architecture Technology Research and Development Systems Requirements Planning Test and Evaluation Systems Development
Operate and Maintain	Data Administration Knowledge Management Customer Service and Technical Support Network Services System Administration Systems Security Analysis
Protect and Defend	Computer Network Defense (CND) Analysis Incident Response CND Infrastructure Support Vulnerability Assessment and Management
Investigate	Digital Forensics Investigation
Collect and Operate	Collection Operations Cyber Operations Planning Cyber Operations
Analyze	Threat Analysis Exploitation Analysis All Source Intelligence Targets
Oversight and Development	Legal Advice and Advocacy Strategic Planning and Policy Development Education and Training Information Systems Security Operations Security Program Management

57. National Initiative for Cybersecurity Education (NICE), "National Cybersecurity Workforce Framework," 2012, http://csrc.nist.gov/nice/framework/.

Appendix 2: Cybersecurity-related Member Organizations and Associations [58]

American Society for Industrial Security (ASIS)
Applied Computer Security Associates (ACSE)
Center for Secure Information Systems (CSIS)
Computer Security Institute
Computing Technology Industry Association (CompTIA)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association, Inc. (ISSA)
InfraGard
International Association for Computer Systems Security, Inc. (IACSS)
International Federation for Information Processing (IFIP) Technical Committee 11 (TC-11) on Security and Protection in Information Systems
International Information Systems Security Certification Consortium (ISC)[2]
International Society for Professionals in E-Commerce (iSPEC)
The IT Governance Institute (ITGI)
The Open Web Application Security Project (OWASP)
SANS Institute (System Administration, Audit, Network, Security)

58. NIST Computer Security Resource Division, "Professional Development," http://csrc.nist.gov/groups/SMA/ate/development.html.

Appendix 3: Certifying Organizations[59]

Advanced Information Security (AIS) Certification
Certified Ethical Hacker (CEH)
Certified Information Systems Auditor (CISA)
Certified Information Security Manager (CISM)
Certified Information Systems Security Professional (CISSP)
Certified Protection Professional (CPP)
Check Point Certified Security Administrator NGX
Check Point Certified Security Expert NGX
Cisco Certified Network Associate (CCNA)
Cisco Certified Security Professional (CCSP)
CompTIA - Security +
CompTIA - A +
CompTIA - Network +
DoD CIO Certificate Program (with Security and Assurance Competencies)
Global Information Assurance Certification (GIAC) Information Security KickStart
Global Information Assurance Certification (GIAC) Level One Security Essentials
Global Information Assurance Certification (GIAC) Level Two subject area modules
Global Information Assurance Certification (GIAC) Security Engineer
Microsoft Certified Professional (MCP)
Security Certified Network Architect (SCNA)
Security Certified Network Professional (SCNP)
System Security Certified Practitioner (SSCP)
Security Leadership, MGMT 512 (GSLC)

59. NIST Computer Security Resource Division, "Professional Development," Ibid. NICE in partnership with the Federal Chief Information Officer's Council, " 2012 Information Technology Workforce Assessment for Cybersecurity: Summary Report," March 14, 2013, http://niccs.us-cert.gov/careers/2012-information-technology-workforce-assessment-cybersecurity-itwac.

Appendix 4: ABET Structure and Education Program Accreditation[60]

ABET Accreditation Commissions:
Computing Accreditation Commission (no reference to degree levels)
Computer Science and Similarly Named Computing Programs
Information Systems and Similarly Named Computing Programs
Information Technology and Similarly Named Computing Programs
Engineering Accreditation Commission (Baccalaureate and Masters)
Program Criteria for Electrical, Computer, Communications, and Similarly Named Engineering Programs
Program Criteria for Software and Similarly Named Engineering Programs
Program Criteria for Systems and Similarly Named Engineering Programs
ABET Cybersecurity-related Member Associations:
CSAB – Computing Sciences Accreditation Board
Lead Society for Computer Science, Information Systems, Information Technology, Software Engineering
Cooperating Society for Biological, Computer, and Information Engineering Technology
In turn, it has two member associations – Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS) - two largest technical, educational, and scientific societies in the computer and computer-related fields
IEEE – Institute of Electrical and Electronic Engineers
Lead Society for Computer, Electrical/Electronic(s), Electromechanical, Information Engineering Technology, and Telecommunications
Cooperating Society for Biological, Bioengineering / Biomedical, Engineering Management, Ocean, and Software
INCOSE – International Council on Systems Engineering
Co-Lead for Systems
ISA – International Society for Automation
Lead Society for Instrumentation and Control Systems
Co-Lead Society for Systems
ABET Accredited Computing-related Education Programs:
Computer Engineering
Computer Science
Information Engineering Technology
Information Systems
Information Technology
Instrumentation and Control Systems Engineering Technology
Software Engineering
Systems Engineering
Telecommunications Engineering

60. ABET, http://www.abet.org/.

About the Pell Center

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Pell's legacy, the Center promotes American engagement in the world, effective government at home, and civic participation by all Americans.

www.salve.edu/pellcenter

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

SALVE REGINA UNIVERSITY