Cyber Certification and/or Licensure?

Kathryn Stephens, NSCI
November 19, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Issues

There has been significant discussion regarding certification and/or licensure of professionals working in the cyber domain, and who should set the associated standards, perform the assessment, issue the certificate/license, etc. The intent of this paper is to look at the similarities and differences, and offer a few observations regarding the way-ahead.

Although certification and licensure share a few key characteristics, they are also very different. Licensure is generally considered a mandatory requirement to practice in a certain profession or occupation. It usually includes a set minimum competence, and is meant to keep incompetent workers from practicing a specific profession. Certification is generally an assessment of a candidate's skills and knowledge that usually includes education or training, and an evaluation. Certifications are meant to formally recognize those who are trained and evaluated in a specific area or subject, and are usually awarded by a private organization that can train and evaluate candidates. On the other hand, licensure is usually overseen by a state government.

The medical industry, for example, has doctors who are educated, typically certified, required to be licensed to practice medicine, and credentialed. For example, following the completion of an appropriate degree by an accredited university or college, certification by the American Board of Medical Specialties is voluntary. This specialty certification involves a "rigorous process of testing and peer evaluation that is designed and administered by specialists in the specific area of medicine."[1] Licensure is done on a state-by-state basis and sets the minimum competency requirements to diagnose and treat patients in a particular state. Following certification and licensure, a doctor is credentialed to practice at specific hospital(s). Other occupations within the medical profession – nurses, medical assistants, and laboratory technicians, for example – have a similar process. These individuals have studied the specific skills required for their position, and have passed an evaluation in order to become certified. An important distinction among all of these is that certification typically follows national standards, is voluntary, includes a peer assessment, and may be specialty-specific. On the other hand, licensure is done at the state level. Both certification and licensure have prerequisite education requirements.

A driver's license is also a good example. A driver's license is issued to all drivers by the state government. A license is the minimum requirement that someone must have to drive. If a driver wanted to become a truck driver, however, they would have to go through additional training and receive certification that would qualify them to be a truck driver. Similarly, cybersecurity experts and officials are calling for the government to develop some kind of national cyber certification program that would help to establish a more skilled cyber workforce in the federal government.

[1] American Board of Medical Specialties; http://www.abms.org/About_Board_Certification/means.aspx; Accessed on 11/17/2010.

Ideas

A recent report from Cisco and (ISC)[2] found that federal chief information security officers now rely more heavily on well-trained and experienced workers to handle technical tasks, since 63 percent of federal CISOs believe their job is becoming more managerial and policy-driven. Seventy percent of the CISOs participating in the survey rated professional certifications as high or very high in importance when hiring and promoting employees, and believe that security certifications should be mandatory for security professionals in government positions.[2]

Pending legislation, such as the Cybersecurity Act of 2009 (S.773), include certification for federal cybersecurity workers. The Cybersecurity Act of 2009 "directs the Secretary to develop or coordinate a national licensing, certification, and recertification program for cybersecurity professionals and makes it unlawful to provide certain cybersecurity services without being licensed and certified."[3]

Section 7 of the Cybersecurity Act of 2009 discusses the proposed federal licensing and certification requirements. The Act says that "within one year after the date of enactment of this Act, the Secretary of Commerce shall develop or coordinate and integrate a national licensing, certification, and periodic recertification program for cybersecurity professionals." The Act also says that "beginning 3 years after the date of enactment of this Act, it shall be unlawful for any individual to engage in business in the United States, or to be employed in the United States, as a provider of cybersecurity services to any Federal agency or an information system or network designated by the President, or the President's designee, as a critical infrastructure system or network, who is not licensed and certified under the program."[4] The bill is currently under consideration in the Committee on Commerce, Science, and Transportation.

Although state level licensure is more common, there are other examples of federal licensure. Some businesses, for example, require federal licensure, and firearms licenses are also handled by the federal government. The Federal Firearms License (FFL) system is administered by the Bureau of Alcohol, Tobacco, Firearms and Explosives (BATFE), an agency of the U.S. Justice Department, and is required under the Gun Control Act.[5] Businesses are required to obtain a federal business license if it is involved in activities that are supervised or regulated by a federal agency, such as agriculture, mining or drilling, nuclear activities, transportation or the distribution of firearms or alcohol. Otherwise, most businesses require only a state license.[6]

Cybersecurity could be added to the list of services or activities that must be regulated by a federal agency, especially if the federal government defines what parts of cyber are critical infrastructure. Then, like nuclear energy or transportation businesses, cyber security businesses would require federal oversight and federal licensure.

The Commission on Cybersecurity for the 44th Presidency has published a report recommending that federal employees and contractors receive ongoing training in cybersecurity. The Commission believes that the federal government should define a set of skills that cybersecurity workers must possess, and then match cybersecurity workers to specialized areas based on their talents. Cybersecurity workers would be certified through an independent body that would test cybersecurity skills and create federal career paths based on those

[2] Ballenstedt, B. (2010, May 6). *Cyber workers need training*. Retrieved June 18, 2010, from NextGov: http://wiredworkplace.nextgov.com/2010/05/training_certifications_key_for_cyber_workers.php?oref=latest_posts

[3] *Bill Summary and Status S.773*. (n.d.). Retrieved June 18, 2010, from The Library of Congress: http://thomas.loc.gov/cgi-bin/bdquery/D?d111:1:./temp/~bduQaD:@@@D&summ2=m&|/home/LegislativeData.php?n=BSS;c=111|

[4] *Cybersecurity Act of 2009*. (2009, April 1). Retrieved July 5, 2010, from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:s773is.txt.pdf

[5] *Federal Firearms Licenses*. (n.d.). Retrieved July 5, 2010, from NRA-ILA: http://www.nraila.org/issues/factsheets/read.aspx?id=70

[6] *Federal Licenses for Regulated Businesses*. (2010, June 25). Retrieved July 5, 2010, from Business.Gov: http://www.business.gov/register/licenses-and-permits/federal-licenses.html

certifications. Some government workers argue that a certification and ongoing testing requirement would make it harder for talent to come into the government. They also say the government should not pay for cybersecurity certifications or the constant exams required to prove that workers are qualified.[7]

In response to the report from the Commission on Cybersecurity for the 44th Presidency, Karen Evans, a member of the commission and former administrator of e-government and information technology at the Office of Management and Budget, said the report recommends extending cybersecurity training to network operators and developers. Critics argue that the government should not be responsible for creating certification requirements that could make it more difficult to hire and retain cybersecurity talent. Last year, the Partnership for Public Service released a report saying that there are four main challenges that threaten the quality of the federal cybersecurity workforce. One of these challenges was the complicated processes and rules that hamper recruitment and retention efforts. “Is adding more training and certification requirements the key to recruiting, retaining and training up a new cadre of cybersecurity workers? Or would introducing such requirements simply add more red tape to the government’s ability to recruit and retain cybersecurity skills, which are already in short supply?”[8]

The Federal Communications Commission is considering a certification program, and is developing a voluntary program that would certify companies’ practices. The FCC proposal would create incentives for service providers to improve their cyber programs, through the voluntary certification program where the FCC defines general objectives for the program and then assesses service providers. FCC opened the proposal for public comment through September 8, 2010.[9]

The Department of Defense recently announced that the EC-Council Certified Ethical Hacker (CEH) certification will be included as a baseline skill requirement for U.S. cyber defenders. The CEH program is now required for the Defense Department’s computer network defenders (CNDs), a specific group within the DoD’s information assurance workforce. The adoption of the CEH certification is part of DoD Directive 8570 Information Assurance Workforce Improvement Program, which was officially instated on February 25, 2010, and provides guidance on information assurance training, certification and workforce management. Military service, contractors and foreign employees must show compliance with the new Certified Ethical Hacker training requirement by 2011. Jay Bavisi, co-founder and president of EC-Council, says that the CEH program is "...one of the most technically advanced certifications on the directive for CND professionals" and will prepare CNDs to combat hackers in real time.[10]

Some IT professionals wonder if a required certification initiative has been effective, or if the Defense Department is spending too much money and time on certification, thus missing out on training to help the military “evolve with the enemy…Men and women are studying to pass tests to keep their jobs rather than applying analytical thinking to the defense of the country.” Readers of the recent Defense Systems story, “New threats compel DOD to rethink cyber strategy,” say that most certification classes have been only slightly technical, and used mainly as marketing for companies that teach the classes. Another commenter pointed out that “some of those best

[7] Aitoro, J. R. (2010, June 4). *Panel to recommend certifications for cybersecurity workforce*. Retrieved June 18, 2010, from NextGov: http://www.nextgov.com/nextgov/ng_20100604_2456.php

[8] Ballenstedt, B. (2010, June 7). *Boosting Cyber Skills*. Retrieved June 18, 2010, from NextGov: http://wiredworkplace.nextgov.com/2010/06/boosting_cyber_skills.php

[9] Long, E. (2010, May 11). *FCC Building Cyber Certification*. Retrieved June 18, 2010, from NextGov: http://cybersecurityreport.nextgov.com/2010/05/fcc_building_cyber_certification.php

[10] *United States Department of Defense Embraces Hacker Certification to Protect US Interests*. (2010, March 1). Retrieved June 18, 2010, from Infosec Island: https://www.infosecisland.com/articleview/3061-United-States-Department-of-Defense-Embraces-Hacker-Certification-to-Protect-US-Interests.html

qualified for the work are those who shun certification and would barely pass any standardized tests because they are not wired for traditional thought."[11]

Daniel Castro, a senior analyst at the Information Technology and Innovation Foundation, recently wrote a column for FCW.com on the topic of federal certification requirements. Castro writes that "If certifications were effective, we would have solved the cybersecurity challenge many years ago" and said although certifications "can help teach workers how to respond to known cyberattacks…workforce training is not certification, and organizations, not Congress, are in the best position to determine the most appropriate and effective training for their workers." The column received many responses, including one comment that said cybersecurity professionals need more internal training on actual incidents and techniques instead of cramming for an exam. An Army civilian said technical expertise will come from becoming familiar with a certain product or technology, not from a generic book of security best practices. Some readers did state certification has its benefits, such as making employees familiar with more technologies than just those they use in their jobs.[12]

International organizations have also recognized the need for increased education and training for all Internet users. Craig Mundie, chief research and strategy officer for Microsoft, recommends implementing a "driver's license" for all Internet users. Mundie explains, "if you want to drive a car you have to have a license to say that you are capable of driving a car, the car has to pass a test to say it is fit to drive and you have to have insurance." Internet users could be required to pass basic security training, show proof of "insurance" such as antivirus protection, and maintain a record without infections.[13] Like a driver's license, this could be done at the state level instead of the federal level.

Critics of a federal cybersecurity license/certification program say that requiring certifications in the cyber security field is difficult because threats and technologies change so rapidly. Experts worry that we are accepting a limited amount of information as sufficient and then closing federal workers off from new technologies and practices. Certainly a recertification program or ongoing training would have to be part of any cyber certification requirement. Experts also believe that if the federal government does require cyber certifications for federal workers, the government should use industry certifications already tested and taught. Critics say the government could not keep up with the private sector in updating and changing certification material, and rewriting certifications would be reinventing the wheel.

Answers

If the federal government is going to mandate a certification/licensure program, as some pending legislation proposes, it would be better for the federal government to initially focus on certification, starting with federal government positions and contracts, specifically those related to our nation's critical infrastructure.

Ensuring a qualified cybersecurity workforce is not as easy as requiring workers to merely pass a certification exam. Although certifications are helpful for ensuring workers understand a certain technology or skill, certifications alone are likely insufficient. If cybersecurity workers are only required to study for an exam, without hands-on training and additional education, they have knowledge - but lack experience and may still not be qualified. The government could use a lab setting to provide hands-on training and simulation exercises for cyber employees. This would be more helpful than just a written exam, and could be required in addition to a certification. In-depth hands-on training, coupled with peer assessment, would help ensure a qualified workforce,

[11] Welsh, W. (2010, February 9). *Certifications no substitute for technical acumen*. Retrieved June 18, 2010, from Defense Systems: http://defensesystems.com/articles/2010/02/09/cyber-strategy-reader-comments.aspx

[12] Monroe, J. S. (2010, January 5). *Certifications: A false sense of security*. Retrieved June 18, 2010, from Federal Computer Week: http://fcw.com/articles/2010/01/11/backtalk-security-certification.aspx

[13] *UN agency calls for global cyberwarfare treaty, 'driver's license' for Web users*. (2010, January 31). Retrieved June 18, 2010, from Prison Planet: http://www.prisonplanet.com/un-agency-calls-for-global-cyberwarfare-treaty-'driver's-license'-for-web-users.html

rather than just a foundational knowledge of cyber security. Periodic re-certification and/or continuing education credits may also be useful to ensure knowledge and skills keep pace with the ever evolving cyber landscape.

The government should consider using certifications that are already available in the private sector. It would be a waste of government resources to duplicate certifications the private sector have in place. The Defense Department, for example, is requiring their CNDs to get the Certified Ethical Hacker certification from the EC-Council as part of the DoD Directive 8570 Information Assurance Workforce Improvement Program. Organizations should identify what skills are most important for their workers, and then match those to skill sets that are already covered by private sector certifications. In the event there are gaps, the organization should request modification of the private sector certification program. There are several organizations currently offering certification and hands-on training employees could attend, including Global Knowledge, SANS, EC Council, and (ISC)^2.

If cyber licensure were left to the states, instead of the federal government, there must be changes to current cyber security standards and practices across states. The licensure program for doctors and lawyers is currently regulated by states, although licensure in multiple states is allowed. Similarly, drivers' licenses are issued from the state, but licenses are valid in multiple states because of common rules and standards across the states. Street signs, speed limits, stop lights, safety requirements and vehicle maintenance standards are the same from state to state. This allows drivers to use their licenses in any state, regardless of which state issues the licenses. Cybersecurity currently lacks common, accepted standards or practices that would enable licensure reciprocity across state lines. In the case of a cyber licensure program, federal legislation may be required to ensure states identify and adopt a minimum set of cybersecurity standards and practices each state could adopt.

Summary

We believe the best approach is to first define the program and associated standards while not getting bogged down in whether it is a certification or licensure. How the program is implemented should be separated from its purpose and objectives.

We also believe the lack of geographical boundaries in the cyber domain necessitates a national (and perhaps international) approach to standards and/or practices. This should be a collaborative effort with states and private industry where the federal government facilitates, but does not dictate the answer. Standards and practices, and the "governance" put in place to identify and maintain them, must accommodate the pace of change in cyber technologies, processes, and operations - or risk being irrelevant and actually hindering progress.

In addition, we believe private industry is in the best position to actually offer the courses, exercises, etc., regarding cyber certification/licensure. They already offer many such opportunities and have consistently demonstrated a responsiveness to government needs.