NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

BEST PRACTICES FOR IMPLEMENTING PROFESSIONALIZATION

Whitepaper

DRAFT

Version 1.0

Last Updated: September 13, 2012

Table of Contents

List of Tables

List of Figures

1 Needs Statement

Evidence continues to demonstrate the vulnerability of the United States' information infrastructure. Military and nuclear energy systems are under continuous attack and have been compromised repeatedly. Over a six year period, the Department of Defense nuclear laboratory sites and other sensitive United States (U.S.) civilian government sites were hacked multiple times. Additionally, terrorists and organized crime groups have exploited information system weaknesses and have extorted money for criminal and terrorist purposes. For example, in October 2008, Express Scripts, one the nation's largest processors of pharmacy prescriptions, reported extortionists threatened to disclose personal and medical information on millions of Americans if the company failed to meet payment demands. More recently, in December 2011, a Wall Street Journal article reported that a group of Chinese hackers broke into the U.S. Chamber of Commerce database and obtained data on its three million members. The breach lasted for at least a year before the Federal Bureau of Investigations (FBI) was able to discover it and alert the Chamber.

As indicated in the Center for Strategic and International Studies' (CSIS) "A Human Capital Crisis in Cybersecurity," the U.S. not only has 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 code, and create the ever more sophisticated tools needed to prevent, detect, mitigate and recover from damage due to system failures and malicious acts. This threat underscores the urgent need for a professionalization process to ensure that qualified cybersecurity professionals are safeguarding the information technology systems and infrastructure of public and private organizations. In order to meet this need, The National Initiative for Cybersecurity Education (NICE) aims to identify professionals with the requisite cybersecurity knowledge, skills, and abilities. As the lead for the NICE Component 3 - Cybersecurity Workforce Structure, the Department of Homeland Security (DHS) strives to increase the quality of the cybersecurity workforce by collaborating with Federal agencies, state, local, tribal and territorial governments, industry, and academia to determine whether and how to professionalize specialty areas within the National Cybersecurity Workforce Framework (hereafter referred to as "The Framework").

2 Purpose of this Paper

The purpose of this paper is to describe best practices for professionalizing cybersecurity specialty areas within The National Cybersecurity Workforce Framework. Because cybersecurity is a young and developing field, this paper examines how more established occupations outside of cybersecurity have been professionalized or are in the process of becoming professionalized. This paper describes a process model of professionalization, based on Curnow and McGonigle's (2006) analysis, which organizes the professionalization process into five major stages. This paper then describes how various occupations have engaged in these stages. Lessons learned and best practices obtained from this review aim to assist DHS and NICE Component 3 in developing criteria for determining whether and how to professionalize The Framework's specialty areas.

3 Defining a Profession

Consistent with previous papers supporting NICE Component 3 (e.g., United States Department of Homeland Security, 2012), this paper adopts Cox's (2010) view that "a profession is defined by: (1) a body of knowledge, (2) ethical guidelines, and (3) a professional organization with a growing set of published papers and best practices" (p. 7). Professionalization refers to the process by which "any trade or occupation transforms itself through the development of formal qualification based upon education, apprenticeship, and examinations, the emergence of regulatory bodies with powers to admit and discipline members, and some degree of monopoly rights" (Bullock and Trombley, 1999). The following sections describe this professionalization process and present real-world examples of occupations that have engaged in various stages of professionalization.

4 The Professionalization Process

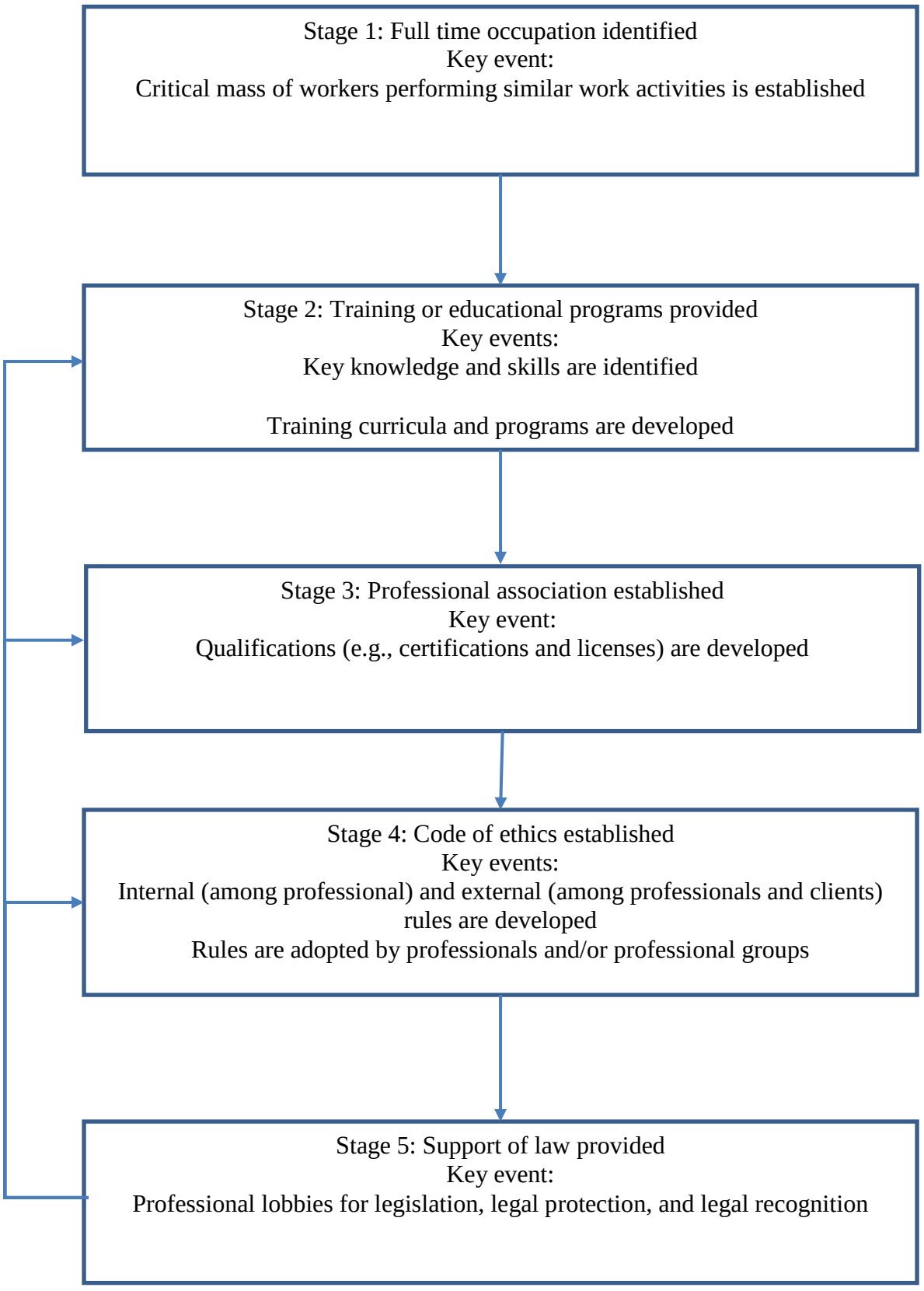
Although work activities may vary greatly from one occupation to another, the professionalization process for occupations is fundamentally the same. According to the process model of professionalization (see Figure 1), occupations occupy different locations on a "continuum" of professionalization where some occupations are more professionalized than are others. The process model of professionalization presents a linear process of one stage leading into the next. However, later stages can also affect earlier stages. If a professional association sets new certification standards, then these standards could change training and education curricula (Curnow & McGonigle, 2006).

Subsequent sections of this paper will describe how various occupations have engaged in each of the stages of the process model of professionalization. Information from these occupations was collected through researched case studies and interviews conducted with subject matter experts (SMEs) who have participated in the professionalization of their occupations or fields. These case studies and SMEs aim to provide supplementary information for this project. They were identified through searches in academic research databases and through the researchers' professional networks. Inclusion of these case studies and SMEs does not represent DHS' or SRA's endorsement of these sources for any purpose other than to supplement the information that is already included in this paper.

The case studies and SME interviews that will be referred to in the sections below include:

- The Department of Defense's (DoD) Security Professional Education Development (SPēD) Certification Program;
- The Department of Veterans Affairs (VA) Information Security Officer (ISO);
- International Information Systems Security Certification Consortium (ISC^2)

Figure 1: Process model of professionalization (Curnow & McGonigle, 2006)



Stage 1: Full time occupation identified

The first stage of the professionalization process is determining whether an occupation exists. An occupation is characterized by a group of workers who perform similar work activities. The specialty area "Information Systems Security Management," which is located in the "Operate and Maintain" category of The Framework, refers to individuals who oversee an information system's information assurance program and who might also be responsible for procuring information technology. Typical job titles associated with this specialty area include "Information Systems Security Officer (ISSO)" and "Information Assurance Manager." Determining whether the specialty area "Information System Security Management" *should* be professionalized is beyond this paper's scope; however, the primary work activities associated with this specialty area, e.g., overseeing an information assurance program and procurement, differentiate this specialty area from the others.

An occupation is identified when a critical mass of workers perform the same or similar work activities. The number of workers that constitute a "critical mass" might vary from one occupation to the next, i.e., there is no one, agreed-upon number of workers, who are performing similar work activities, which must be obtained before an occupation can be identified. Occupations arise in response to a need for individuals to perform a given set of activities. Doctors and lawyers have existed for hundreds of years in response to the need for medical treatment and legal services. The need for an occupation might also arise in response to technological advancements. The advent of the airplane heralded the rise of the aviation field and the occupations that it contains, such as pilots, air traffic controllers, and aeronautical engineers. Similarly, the advent of the Internet heralded the rise of diverse new occupations, such as web developers, security engineers, and, of course, cybersecurity professionals.

Stage 2: Training or educational programs provided

The second stage of the professionalization process is developing training and educational programs. To develop training and educational programs, the knowledge and skills that are required to perform the occupation's core work activities must be identified. These are typically summarized in a Body of Knowledge (BoK), although not all occupations possess a formal BoK. Continuing with the current example, the knowledge and skills that are required to perform the work activities for "Information System Security Management" must be identified in order to create valid training and educational programs.

Occasionally, a significant adverse event prompts organizations to engage in this stage of professionalization. The Department of Veterans Affairs (VA) professionalized its cybersecurity workforce after an ISSO's laptop was reported missing. The Department of Defense (DoD) began its effort to professionalize cybersecurity workers after several investigations identified a lack of consistency in its security training program. Finally, the International Information Systems Security Certification Consortium (ISC^2) professionalized the cybersecurity occupation after unqualified practitioners performed their work unsatisfactorily, thereby jeopardizing the cybersecurity field's reputation.

An established training program holds significant importance in reducing the number of errors, fraud, and abuse to organizational assets. Furthermore, it enhances the skills, capabilities, and knowledge of employees for performing a particular job. The Department of Defense's (DoD) Security Professional Education Development (SPēD) Certification Program is a DoD-wide training and certification program that provides its information security professionals with a path toward professionalization and establishes standardized competencies across DoD Services and commands.

The SPēD Certification Program is a four-level certification program that is predicated on establishing skill standards and job competency requirements that were developed and approved by the DoD Security Training Council. In addition, the SPēD Program identified 16 security competencies with associated knowledge categories. These requirements are supported by a curriculum that provides information security practitioners with the requisite training to become proficient in their areas of expertise and ensure that information security personnel have the competencies to fulfill the identified security accountabilities.

Before launching its first Certified Information System Security Professional (CISSP) exam, which is an examination that tests the principle knowledge and experience of information security professionals covering 10 domains[1], ISC^2 developed a common body of knowledge to provide a framework of terms and principles for information security professionals to communicate and ensure a common understanding.

Stage 3: Professional association established

The third stage of the professionalization process is establishing a professional association. A professional association develops and manages certification and licensure standards that identify qualified workers. Such standards provide assurance that individuals are able to perform the occupation's work activities. The founders of ISC^2 established its association after identifying a lack of professionalism within the information security field. Unqualified individuals, who claimed to be able to perform cybersecurity responsibilities, began to reflect badly on the cybersecurity industry. The ISC^2 founders wanted to create a known profession and needed to establish the standards to do so. Similarly, certification for an individual, who performs work

[1] The CISSP certification covers the following 10 domains: Access Control, Telecommunications and Network Security, Information Security Governance and Risk Management, Software Development Security, Cryptography, Security Architecture and Design, Security Operations, Business Continuity and Disaster Recovery Planning, Legal, Regulations, Investigations and Compliance, and Physical (Environmental) Security.

within The Framework's "Information System Security Management specialty area, would provide proof to that individual's ability to oversee an information assurance program and procure the requisite information technology equipment.

Stage 4: Code of ethics established

The fourth stage of the professionalization process is establishing a Code of Ethics. A Code of Ethics, which is typically enforced through the occupation's professional association, determines the rules that govern how occupations members interact with one another and with clients. A Code of Ethics helps an occupation establish and enforce professional norms. A Code of Ethics is especially relevant to cybersecurity because cybersecurity professionals are charged with protecting data networks and infrastructure. Not only must these professionals possess the technical skills to perform this work, but they must also possess the motivation to perform this work. Lack of effort or ethical lapses in performing this work can lead to serious cybersecurity breaches. A famous historical example of how human fallibility can exploit a defense system is when the Mongols invaded China simply by bribing a sentry to let them pass through a gate of the Great Wall of China. Similarly, the best cybersecurity defenses are compromised if the people who are responsible for them are unethical.

Stage 5: Support of law provided

The fifth stage of the professionalization process is obtaining the support of law, which includes legislation, legal protection, and legal recognition. This stage of the professionalization process is important for occupations to be perceived as legitimate and to promote the occupation's interests. Occupation members form coalitions, associations, or organizations to pursue, monitor, and evaluate legislation that affects the occupation.

In the information technology field, monitoring legislative developments is especially important since legislation must attempt to keep pace with technological innovations that continuously change the field. Numerous organizations examine pertinent issues related to information technology law and, in particular, examine how information technology legislation affects information technology professionals. Such organizations include, for example, EDUCAUSE.

EDUCAUSE monitors information technology legislation and develops information technology policies for institutions of higher learning that are in accordance with this legislation.

EDUCAUSE examines how changes in the law affect information technology professional development. The Information Technology Law Association (ITLA) was founded to educate lawyers on unique legal issues related to the development and implementation of information technology. In increasing awareness of these issues among lawyers, information technology professionals have a voice in shaping legal issues and development that affect their profession. As the cybersecurity field matures, its members will likely need to form organizations, or to partner with existing organizations, that pursue favorable cybersecurity legislation.[2]

5 Aviation and Cybersecurity Similarities

Thus far, this paper has reviewed case studies that examine how various occupations have engaged in various stages of the professionalization process in an effort to provide insights into how cybersecurity might be professionalized most effectively. This section describes general similarities between occupations in the fields of aviation and cybersecurity in an effort to illustrate further approaches to professionalizing cybersecurity.

To become a pilot, an individual must possess a pilot license. Although a pilot license might appear straightforward at first glance, pilot licensure spans many levels and certifications (see Table 1). For example, the standards for obtaining a Student Pilot license are minimal, whereas airline pilots must have a fundamental understanding of physics, meteorology, navigation and geography, must pass a strict physical exam to ensure they are in good health, and must have vision that is correctable to 20/20, as well as no physical handicaps that could impair their performance. In addition, airline pilots must pass a written test, and demonstrate their flying ability to a Federal Aviation Administration (FAA)-designated examiner.

Similarly, cybersecurity certifications or licensures must reflect the type of work that the person must perform and the context in which the person must perform this work. Most likely, a self-employed person, who builds a small business website, does not need advanced cybersecurity certifications since the ramifications of a cybersecurity breach are likely minimal, i.e., they would impact only this person and his or her clients. In contrast, a person, who is responsible for ensuring the data integrity of a classified government database, would likely need advanced

[2] See Appendix for a detailed example of how a field unrelated to cybersecurity pursued and obtained legal recognition and support.

certifications and licensure as a testament to this person's ability to protect data systems. In contrast to a small business owner's cybersecurity breach, a cybersecurity breach of a classified government database could have serious national security implications. Like the pilot occupation, where licensure standards tend to increase in proportion to the number of passengers for which the pilot is responsible, the licensure standards for cybersecurity professionals might also increase in proportion to the magnitude of the ramifications of a cybersecurity breach.

Minimum knowledge and skills are required by all pilots regardless of the pilot's level of certification, such as the ability to read, speak and understand the English language, and to exercise reasonable judgment, which is indicated by the minimum age requirements to become a pilot. However, as a pilot pursues more advanced licenses, the knowledge, skill, and certification requirements increase. An Airline Transport Pilot is authorized to fly large aircraft with hundreds of passengers, whereas a Sport Pilot is limited to carrying only one passenger, must fly during the daytime, and must remain below 10,000 feet. Similarly, a required skill level for all cybersecurity professionals can be determined for the cybersecurity field. Currently, most organizations require cyber professionals to possess a four-year bachelor's degree; however it is not required by all.

Table 1: Overview of Pilot Standards and Qualifications

Type of Pilot	Age	Language Skills	Medical Status	Knowledge & Flight Tests	Flight Time
Student	Must be at least 16 years old	Read, speak and understand English	Hold at least a current 3rd class medical certificate / complete physical examination	N/A	N/A
Sport	Must be at least 17 years old	Read, speak and understand English	Must hold either a 3rd class medical certificate or U.S. driver's license	Pass FAA Sport Pilot Knowledge & Practical Test	Complete 15 hours of flight instruction / Complete 5 hours of SOLO practice flying
Recreational	Must be at least 17 years old	Read, speak and understand English	Hold at least a 3rd class medical certificate	Must pass both a written knowledge test and a flight test	Complete 15 hours of SOLO practice flying
Private	Must be at least 17 years old	Read, speak and understand English	Hold at least a 3rd Class Medical Certificate	Pass the FAA knowledge test Receive endorsements from a CFI for both knowledge and practical tests	At least 40 hours flight time / 20 hours of SOLO experience
Commercial	Must be at least 18 years old	Read, speak and understand English	Hold at least a Pilot Certificate	Pass required knowledge test on aeronautical areas / pass practical test	Complete 250 flight hours (single-engine) / Complete 150 flight hours (helicopter)
Airline Transport	Must be at least 23 years old	Read, speak and understand English	Hold at least a current 3rd class medical certificate	Possess a commercial pilot w/instrument rating / pass a knowledge test with a score of 70% or better / complete a practical test	Complete at least 1,500 hours of flight time / Complete 500 hours of cross-country Complete 100 hours of night time or 75 hours+ 45 full stop landings Complete 75 hours instrument flight time, or 50 flight + 25 simulator

6 Methodology for Determining a Specialty Area

How does an organization, or a collection of practitioners, decide whether to professionalize an occupation? Although there are many possible answers to this question, a common denominator is that the decision to professionalize depends on the need to verify the quality of the services that the occupation provides.

Professionalization focuses on verifying that individuals have the knowledge and skills they need to perform an occupation's tasks. Specific steps toward this goal include identifying the tasks that must be performed, creating a Body of Knowledge, and developing certification and licensure requirements. Looking at The Framework, a likely specialty area that may need to be professionalized is Software Engineering due to the growing number of cyber attacks. The Framework defines a software engineer as one who "develops, creates, and writes/codes new (or modify existing) computer applications, software, or specialized utility programs." This specialty area includes roles such as Computer Programmer, Web Application Developer, and Software Developer, and is deemed a critical area as previously discussed in the CSIS report.

Another specialty area likely to professionalize is the Information Systems Security Management which was demonstrated in the VA OIT case study.

Professionalization also involves the support of legislation and professional associations to oversee credentialing, as well as enforcing a code of ethics. A profession engages in legislative support for legal protection and restrictions, and recognition of title and work activities. This was demonstrated in the interior design case study. A code of ethics provides rules for governing the relationships of a profession both internally (one professional to another) and externally (professional to a client).

7 Conclusion

The purpose of this paper was to identify best practices for professionalizing the field of cybersecurity. Given cybersecurity's importance to national security, having a professional cybersecurity workforce that can demonstrate proficiency is critical. This paper reviewed two professionalization case studies and two interviews with SMEs, who have been engaged in professionalizing occupations, related to information security, and applied these examples to a process model of professionalization. The process model aims to guide professionalization initiatives by organizing the professionalization process into a logical framework.

This paper also explored similarities between aviation and cybersecurity occupations. Just as pilots must meet stricter training and certification standards as they fly larger airplanes, transport more passengers, and travel greater distances, so too might cybersecurity professionals need to meet stricter training and certification standards as they perform work that demands greater information security. While pilots and cybersecurity professionals must have advanced knowledge and skills in order to perform their occupations' most complex responsibilities, these occupations also have minimum knowledge and skill requirements that apply to all members of these occupations. Across the board, pilots must be able to speak, read, and write English, and the minimum age requirement suggests that pilots must also possess reasonable judgment.

Similarly, cybersecurity professionals likely will need to possess minimum language, judgment, and information technology-related skills regardless of the type of cybersecurity work they perform.

This research yielded a list of best practices for successfully implementing cybersecurity professionalization such as obtaining buy-in from senior management, and having appropriate funding. Gaining support from stakeholders also influences whether a project succeeds or fails. A next step will require the identification of cybersecurity specialty areas to professionalize. This paper mentioned two such specialty areas, which are likely to be professionalized. We hope this research provides guidance for implementing cybersecurity professionalization.

Acronyms

Acronym	Definition
CSIS	Center for Strategic and International Studies
DHS	Department of Homeland Security
DoD	Department of Defense
DoDIG	Department of Defense Office of Inspector General
DSS	Defense Security Service
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigations
ISC^2	International Information Systems Security Certification Consortium
ISO	Information Security Officer
ISSO	Information Systems Security Officer
IT	Information Technology
ITWD	Information Technology Workforce Development
NCIDQ	National Council for Interior Design Qualifications
NICE	National Initiative for Cybersecurity Education
OIT	Office of Information Technology
OPM	Office of Personnel Management
OUSD(I))	Office of the Under Secretary of Defense for Intelligence
SMEs	Subject Matter Experts
SPēD	Security Professional Educational Development
U.S.	United States
USD(I))	Under Secretary of Defense for Intelligence
USPS	United States Postal Service
VA	Veteran Affairs

References

"2011 Cyber Attacks Timeline Master Index," last modified July 6, 2012, http://hackmageddon.com/2011-cyber-attacks-timeline-master-index/

"About EDUCAUSE," last modified August 20, 2012, http://www.educause.edu/

"About ITechLaw," last modified August 20, 2012, http://www.itechlaw.org/

Bullock, A. & Trombley, S. (1999). The New Fontana Dictionary of Modern Thought, Londone: Harper-Collins, 689.

Center for Strategic International Studies. 2010. A Human Capital Crisis in Cybersecurity, Technical Proficiency Matters, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. 2010

Cox, L. (2010). Creating a profession and a body of knowledge for product supportability engineering at high-tech companies. (Doctoral dissertation). Retrieved from ABI-Inform database.

Curnow, C. & McGonigle, T.P. (2006). The Effects of Government Initiatives of Occupations, Human Resource Management Review. 286-292.

Federal Aviation Administration (FAA), 2012. Licenses & Certificates. Accessed July 16, 2012. http://www.faa.gov/licenses_certificates/

United States Department of Homeland Security (DHS) (2012). A Historical Review of How Occupations Become Professions.

U.S. Department of Defense, Office of Inspector General. 2011. Assessment of Security Within the Department of Defense – Training, Certification, and Professionalization. Washington, DC: Government Printing Office, 2011.

U.S. Department of Veterans Affairs, Office of Information Technology. 2011. Guide to Developing a VA OIT Competency Model – Best Practices Document. Washington, DC: Government Printing Office, 2011.

Whitney, Marilyn Corsen, "A History of the Professionalization of Interior Design" (PhD dissertation, Virginia Polytechnic Institute and State University, 2008).

Appendix

Legislation Case Study: Interior Design

Although cybersecurity and interior design are unrelated, the interior design occupation provides a valuable case study for how cybersecurity might pursue legislation and other legal initiatives. Approximately 20 interior designers, who formed a coalition in Washington, DC, saw the need for interior design to become a recognized profession. The mission of the coalition was to become the leaders and impetus for licensing in the U.S. The coalition hired an attorney who worked for the National Council for Interior Design Qualifications (NCIDQ), to begin drafting a bill.

Members of the coalition testified at public hearings emphasizing the importance of their profession, and how a licensed interior designer could improve "the health, safety, and welfare of the public." The Congressional review approved the bill on the first vote, and the mayor signed it into law. After the first few years, over a thousand interior designers became licensed. The critical aspect of this particular case study is that it describes the interplay between a group of practitioners and legislators. This case study underlines practitioners' dependence on legislators for legal recognition and protection. The case study on interior design traces the professionalization process of interior designers from inception to lobbying Congress in formulating the first practice legislation for interior design in the United States. Eventually, cybersecurity professionals might also require legislative support, which may require a course of action similar to that taken by the interior design occupation.