Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

An Analysis of the State of Cyber Security Education in America

W.V. Maconachy, PhD. *Fellow of ISC*^{2}, Jennifer Duryea, and Peter Starland, *Capitol College*

Abstract – This paper discusses the need to develop a common understanding of a curriculum which prepares students to practice in the field of Information Assurance (IA). A study of public documents, congressional hearings, published papers and conference presentations regarding the state of cyber security in America was conducted to discover commonality regarding cyber security education and training. The document review discovered, within academia, information assurance education is not consistently approached; there is a lack of definition and corresponding need for specificity regarding information assurance curriculum. Furthermore, a nearly decade long government call to action for academia to produce increasing numbers of information assurance professionals may not have come to full fruition. However, we found no evidence of a well-defined plan of action to reach this desired goal. The authors propose a national summit to address information assurance education at the graduate and undergraduate level.

Index terms – cyber security education, information assurance curriculum, information assurance education.

I. Introduction

A. Purpose

The investigators ask the question, "How far and in what direction has information assurance education evolved within the last decade?" Hentea and Dhillon in their 2006 study, "Towards Changes in Information Security Education," concluded that: "So far, government and professional organizations, and employers of ISA [Information Security Assurance] specialists have been the drivers of the ISA curricula and programs at our universities. There are numerous ISA education models and curricula in existence at educational institutions around the world. The market place for the products, services, and personnel is now global, and ISA curriculum should be based on national and international standards"[1]. The scope of our study was delimited to progress made in information assurance education within the U.S. The terms information assurance and cyber security were used synonymously in the documents reviewed and will therefore be used interchangeably in this paper.

B. Background

U.S. Government agencies and a host of industry experts continue to emphasize the need for an increased number of information assurance professionals. Many government reports have cited the lack of properly trained and educated personnel as creating a vulnerability to America's critical information infrastructures [2][3][4][5]. In the 1950s, with the launch of Sputnik, America found itself in the Space Race. As we now enter into a new millennium, America has found itself in a similar cyber security race.

In response to the Space Race, America turned to academia to start producing the engineers, technicians and technology needed to secure and advance our position in space [6]. Now, in the Information Age, America is turning to academia and industry with an urgent need to produce much needed cyber security professionals to secure cyberspace. The government has responded by implementing a few programs to stimulate the study of information assurance within higher education.

This investigation documents the government calls for action and subsequent academic and industry response to produce a national cadre of cyber security professionals. In 2008 Department of Homeland Security (DHS) Secretary Chertoff inferred that a lack of trained professionals in the life cycle development process of information technology/systems may be a leading cause of cyber security vulnerabilities. He made the following statement at the Cyber Strategic Inquiry conference, "…We have to defend against the full spectrum of threats by having a serious look at our counterintelligence approach -- in other words, how do we make sure that people aren't compromising our system from within -- and also by looking at the security of the supply chain because some of the threats that we're experiencing to the internet don't come by people coming in over the network. They come by people corrupting the hardware and software that is of course that architecture through which the internet operates"[7].

II. Methodology

This paper reviews 41 documents concerning IA education. The documents, dating back to 1998, included

government reports, public source briefings, formal papers, etc. See Appendix A.

The Committee for National Security Systems (CNSS), National Institute of Standards and Technology (NIST), and Office of Personnel Management (OPM) information security glossaries were used to compile a list of ten keywords. These terms were selected because they appeared most commonly between the sources. Upon selection, the number of occurrences of each term was recorded for each document. The results of this keyword search are found in Appendix B. It is interesting to note that, as shown in Appendix B, the three keywords with by and far the largest hits are: training, threat, and attack.

The next step in the analysis was to take the initial results and focus on elements within those documents which addressed cyber security training and education. The investigators specifically searched for any recommendations regarding the scope, direction, or actions to date in implementing information assurance education. The aggregated results and recommendations, found as a result of the document review, were segmented into three categories: government, industry, and academia.

III. RESULTS

Listed below is the aggregation of actions and recommendations taken to date in cyber security education within government, industry, and academia.

Category A: Government

A review of nine Department of Homeland Security (DHS) reports yielded instances of calls for increased emphasis on IA education and training without specific recommendations as to direction. The DHS Sector-Specific Plans made reference that in order for the security of the nation's critical infrastructures and key resources to be upheld, individual and organizational training and education must be standardized and improved. However, no specific strategy as to how this should be undertaken was made. A summary of those findings is found below. (See Appendix A.4 for complete citation).

Department of Homeland Security Agriculture and Food Sector-Specific Plan, p. 54: "The Food and Agriculture Sector security partners currently support a variety of training and educational activities, including joint exercises; however, much more could be done….use the HSIN-CS to advertise these opportunities."

Department of Homeland Security Communications Sector-Specific Plan, p. 78: "The [National Communication Sector] NCS recognizes the need for training and education in all areas of the [*National Infrastructure Protection Plan*] NIPP Framework … This includes specialized training on risk management methodologies, related to physical and cyber security risk assessments … as the [Sector-Specific Plan] SSP is implemented, there will be a need for expertise in areas where it does not exist."

Department of Homeland Security Water Sector-Specific Plan, Sec 1:96, p. 108: "Successful implementation of the national risk management framework relies on building and maintaining individual and organizational CI/KR protection expertise. Training and education in a variety of areas is necessary to achieve and sustain this level of expertise."

Department of Homeland Security Defense Industrial Base Sector-Specific Plan, Sec 2:41, p. 50: "DoD understands that a successful [Defense Industrial Base] DIB risk management effort requires effective training, education, and outreach. DoD seeks to expand those efforts and support DIB Sector security partners in expanding their education and training."

Department of Homeland Security National Monuments and Icons Sector-Specific Plan, Sec 1:50, p. 58: "Successful implementation of the national risk management framework relies on building and maintaining individual and organizational expertise in CI/KR protection. Training and education at a variety of levels and in a variety of subject areas are necessary to achieve and sustain an optimal level of expertise. … Individual and organizational training as well as tabletop exercises are integral to improving the [National Monuments and Icons] NMI Sector's overall security posture."

Department of Homeland Security Energy Sector-Specific Plan, Sec 1:60, p. 70: **"**Successful implementation of the national risk management framework relies on building and maintaining individual and organizational CI/KR protection expertise. Training and education in a variety of areas are necessary to achieve and sustain this level of expertise."

Department of Homeland Security Transportation Systems Sector-Specific Plan, Sec 2:91, p. 105: "The Transportation Systems SSP SBRM framework cannot be accomplished without robust training and continuous education to expand and augment organizational and individual CI/KR protection expertise. Transportation Systems Sector security partners would greatly benefit from continued training and education on many security-related areas, such as risk evaluation and assessments, response and recovery, and other CI/KR security-related topics."

Seven Government Accountability Office (GAO) reports, (see Appendix A.3), were reviewed and yielded a similar call for an increased emphasis on emphasis and training without specific recommendations as to direction. A GAO report from July 2008, GAO-08-588: *Cyber Analysis and Warning DHS Faces Challenges in Establishing a Comprehensive National Capability*, is representative of the findings and recommendations found in the previous GAO reports, it notes: "…a DOD official representing one of its cyber analysis and warning centers stated that its analysts must develop their expertise on the job because there is no formal training program available that teaches them how to detect and perform analysis of an anomaly or intrusion. A private sector official stated that while analysts are often trained to use existing tools, their understanding of the key attributes of analysis is often limited, resulting in a solution too late to be helpful"[8].

DoD Directive 8570: represents the Department of Defense's leadership in defining workforce roles of information assurance professionals [9]. The DoD has accepted the use of commercial off the shelf certifications as evidence of information assurance knowledge mastery for specific jobs. See Appendix C. The implementing manual, (DoD 8570.01-M), goes farther in actualizing a department-wide IA professional program by establishing metrics and implementing standards [10]. DoD 8570.01-M puts into place a robust IA workforce management program [11]. This is the first federal agency to institute a pervasive IA workforce program.

Committee for National Security Systems: exhibited an exhaustive listing of performance based/job based knowledge skills and abilities for people working on national security systems [12]. Total number of documents in CNSS: 6 instructions and 1 directive all appeared to be regularly reviewed refreshed with exception of 4011. An inquiry to the CNSS community resulted in the discovery that a new CNSS 4011 is currently under review for concurrence. (CNSS representative, personal communication, January 2009). See Appendix A.2.

DHS: *Essential Body of Knowledge*: an unaccredited compilation of IT security roles and corresponding expected competencies and skills presented in a broad manner in an attempt to provide a general framework from which government and industry may draw in the creation of specific occupations as well as professional development programs [13].

NIST 800-16: *Information Technology Security Training Requirements: A Role- and Performance-Based Model*: this 1998 document was "designed as a 'living handbook' to have the longest useful life possible as the foundation of and structure for 'do-able' training by Federal agencies" [14].

NIST 800-50: *Building an Information Technology Security Awareness and Training Program*: "provides guidance for building an effective information technology (IT) security program and supports requirements specified in the Federal Information Security Management Act (FISMA) of 2002 and the Office of Management and Budget (OMB) Circular A-130, Appendix III"[15].

NIST 800-100: *Information Security Handbook: A Guide for Managers Recommendations of the National Institute of Standards and Technology*: "This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program"[16]. The handbook also addresses information security awareness and training[17].

The National Infrastructure Advisory Council's *Workforce Preparation Education and Research Working Group Report* iterated the following recommendations: "C-2 Designate a privately administered, public-private IA training certification body. This can be an existing non-profit organization or a newly established and funded one. This contract organization should develop standardized approaches to IA training, accreditation, certification, testing, metrics, feedback and ongoing improvement" and "Federal government must first address if it is to improve its cyber security efforts effectively. …In researching these points, it is apparent that in addition to these topics, there is another overarching issue: the need for a central coordinating body" [18].

President's Information Technology Advisory Committee's (PITAC) *Cyber Security: A Crisis of Prioritization* "…recommends that the Federal government intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities, with a goal of at least doubling the size of the civilian cyber security fundamental research community by the end of the decade…"[19].

National Infrastructure Protection Plan (NIPP): this 2009 document, with its 18 supporting sector-specific plans, called for multidimensional public private sector partnerships in securing the broader national infrastructures. The document noted that the "Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CIKR [Critical Infrastructures and Key Resources]" [20]. Also, in regards to education, the plan referenced the DHS as supporting "cybersecurity training, education, and awareness programs by educating vendors and manufacturers on the value of: pre-configuring security options in products so that they are secure on

initial installation; educating users on secure installation and use of cyber products; increasing user awareness and ease of use of the security features in products; and, where feasible, promotion of industry guidelines" [21].

The Federal Information Security Management Act (FISMA): "was passed by Congress and signed into law by the President as part of the E-Government Act of 2002 (Pub. L. No. 107-347). The goals of FISMA include development of a comprehensive framework to protect the government's information, operations, and assets"[22]. This act of Congress requires each Federal Chief Information Officer to provide, "training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities"[23].

National Science Foundation (NSF) Scholarship for Service Program: this congressionally funded program provides graduate and undergraduate scholarships for students to study in the field of information assurance. The program also provides funds for colleges and universities to improve their cyber security education infrastructure [24].

The National Centers of Academic Excellence program: this program has been referenced as positive step. "A Study of Security Education in the Era of Cyber-Terrorism," stated the following, "Clearly, security education designed from criteria of the Center of Academic Excellence in Information Assurance program is a helpful, if not critical, component in fighting cyber-terrorism"[25]. In a study by Dark, et al., "Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice," the National Centers of Academic Excellence in Information Assurance Education are referred to as "The most significant effort to involve colleges and universities..."[26].

In summary, government documents which addressed cyber security education (1) demonstrated a consistent recognition and call for action to improve cyber security education, (2) showed leadership in implementing studies and programs which bring definition to the information assurance field, and (3) implemented government funded scholarships and recognized programs of study.

Category B: Industry

SysAdmin, Audit, Network, Security Institute (SANS): this company is a commercial provider of cyber security training based upon its own corporate and instructional staff knowledge of information security.

International Information Systems Security Certification Consortium $(ISC)^2$: has developed its own body of knowledge: the *$(ISC)^2$ Common Body of Knowledge* (CBK).

Computing Technology Industry Association (CompTIA): "CompTIA has developed specialized initiatives and programs dedicated to major areas within the IT industry. They include convergence technology, e-commerce, IT training, software services, certification, public policy and workforce development"[27]. The course content is developed by the CompTIA organizations and validated by subject matter experts.

Center for Strategic and International Studies (CSIS): this study called for the formation of an accreditation body. In the CSIS's report, *Securing Cyberspace for the 44th Presidency*, the following statement was made, "…an accreditation body similar to the Federal Law Enforcement Training Accreditation or the Council on Occupational Education needs to be established that will provide the oversight to guarantee that all federal training centers offering cyber training adhere to quality, effectiveness, and integrity standards…"[28].

In summary, corporations such as $(ISC)^2$, SANS, and CompTIA have researched and formulated industry based programs of study and certification exams in information assurance.

Category C: Academia

A Curriculum Model Based on the SIGITE Guidelines: Discovered use of an IA model being suggested by Special Interest Group for Information Technology Education (SIGITE) and implemented at a few schools [29]. The model cited by Kamali, et al, *A Model for Information Assurance: An Integrated Approach*, proposes an integrated view of information assurance using a four dimensional plane of reference, as found in Figure 1[30].

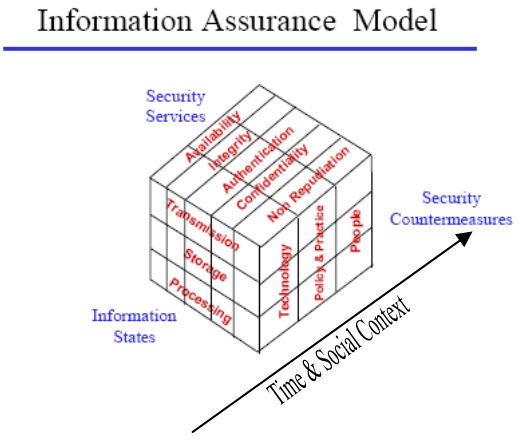


Figure 1

In citing this model as a frame of reference (Gesthalt) for understanding information assurance, the Association for Computing Machinery (ACM) may actually be introducing an approach to producing a comprehensive information assurance curriculum.

ACM Computer Security Curriculum Focus Group: Under the auspices of the ACM, this group has been meeting since 2004 and producing papers which report a wide variety of computer security curriculum models. Most of the curriculum papers demonstrate how computer security/information assurance has been integrated into already existing curriculum [31].

Computing Curricula Information Technology: This ACM document recommends 23 core hours of study in information assurance education as part of an accredited IT degree program [32].

National Security Agency Department of Homeland Security Centers of Academic Excellence (NSA DHS CAE): This program recognizes 94 universities, all with unique curriculum, using CNSS Instruction 4011 as the basis for the common core curriculum [33]. See Appendix A.2.

In summary, colleges and universities across America appear to be in the early stages of moving towards a common curriculum in information assurance education.

IV. Findings and Conclusions

When government or industry hire a computer scientist there is a clear set of expectations regarding the computer scientist's knowledge set, the same applies for engineers, mathematicians, chemists, and a whole host of occupations. In December 2008, the DHS *Essential Body of Knowledge* noted "Variations in training, expertise, and experience are the natural consequences of this evolution, and are reflected in the abundance of recruiting, education, and retention practices among employers"[13]. The DHS "worked with experts from academia, government, and the private sector to develop a high-level framework that establishes a national baseline representing the essential knowledge and skills IT security practitioners should possess to perform"[13]. This DHS document focused on security competencies required within the IT workforce.

The practice of information assurance transcends a variety of jobs. The need for information assurance knowledge and skills has been called for in professions such as computer science, electrical engineering, technical management, and others. We found the beginnings of the definitions for information assurance knowledge and skills emerging within a few disciplines. This common set of expectations has been established by professional accreditation societies such as ACM and ABET. In the ACM 2008 *Information Technology Curriculum Guidelines*, information assurance education is presented using the Maconachy et al. model [34]. However, there appears to be no commonly accepted and agreed upon set of expectations for work competencies required of an information assurance professional. Within academia, as noted by Dark, Ekstrom and Lunt, "Information Technology is maturing rapidly as an academic discipline…we believe that a weakness in many computing programs is the treatment of security topics throughout the curriculum" [35]. This treatment discussed by Dark, et al. is representative of the most common approach to teaching information assurance. That approach is to infuse information assurance topics into already existing curriculum.

There is a growing body of evidence which indicates that information assurance is a multidisciplinary field of study, almost unto itself [36][37][38][39].

The document review produced the following findings:

- With the exception of CISSE, which meets once a year, there appears to be no national coalescing to define the information assurance professional.
- In the government area most work focused around defining jobs, developing training, and seeking commercial off the shelf certifications
- In the industrial area most work centered on certifications and testing.
- No evidence that either a professional society or a group of industry academia and government have come together to define a true information assurance curriculum. This conclusion is supported by Dr. Dark of Purdue, "At this time, I am unaware of any other national effort to formalize the content of information assurance" (M. Dark, personal communication, February 22, 2009).

V. Summary

There appears to be sufficient evidence to support a national call for coalescence among industry, academia, and government to begin defining academic curriculum for the development of an IA professional which is not tied to, nor a subspecialty under, an existing curriculum, (e.g., CS, EE, IRM, etc.). One vehicle proven to be effective in producing this level of collaboration might be a national summit for defining information assurance curriculum. Since the GAO reports and other government documentation indicate that the lack of sufficient numbers of information assurance professionals creates a vulnerability in critical information systems, the U.S. government may well be the best facilitator for such a

dialog. Ultimately, work done at a national summit needs to be incorporated into a global effort for advancing information assurance education.

VI. References

[1] Henta, Marianna and Dhillon, Harpol. (2006). Towards Changes in Information Security Education. *Journal of Information Technology Education, 5*, 230.

[2] President's Information Technology Advisory Committee. (2005). *Cyber Security: A Crisis of Prioritization.* Arlington, VA: National Coordination Office for Information Technology Research and Development.

[3] National Association of State Chief Information Officers. (2007). *Insider Security Threats: State CIOs Take Action Now!*. Lexington, KY: NASCIO. Retrieved from http://www.nascio.org/publications/documents/NASCIO-InsiderSecurityThreats.pdf

[4] Office of Management and Budget. (2007). *Fiscal year 2007 FISMA Report to Congress on Implementation of The Federal Information Security Management Act of 2002*. Washington, D.C.: Office of Management and Budget.

[5] CSO Online. (2008). *5 Must-Do Cyber Security Steps for Obama*. Retrieved February 19, 2008, from http://www.csoonline.com/article/467864/_Must_Do_Cyber_Security_Steps_for_Obama

[6] Office of Science and Technology Policy. (1958). *National Defense Education Act of 1958.* Washington, D.C.: Institute for Defense Analyses Science & Technology Policy Institute.

[7] Chertoff, Michael. (2008, December). *Remarks by Secretary Michael Chertoff at the Cyber Strategic Inquiry 2008*. Speech presented at Ronald Reagan Building and International Trade Center, Washington, D.C.

[8] United States Government Accountability Office. (2008 July). *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*. Washington, D.C.: United States Government Accountability Office. p. 49.

[9] U.S. Department of Defense. (2004). *Information Assurance Training, Certification, and Workforce Management (DoD Directive 8570.01).* Retrieved February 26, 2009, from ttp://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf

[10] U.S. Department of Defense. (2005). *Information Assurance Workforce Improvement Program (DoD 8570.01-M).*

[11] Ibid. pp. 48 – 51.

[12] The Committee on National Security Systems. Retrieved February 18, 2009, from http://www.CNSS.gov/issuances.html

[13] U.S. Department of Homeland Security. (2008). *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development.* Washington, D.C.: U.S. Government Printing Office.

[14] National Institute for Standards and Technology. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model (*NIST SP800-16). p. iii.

[15] National Institute for Standards and Technology. (2003). *Building an Information Technology Security Awareness and Training Program (NIST SP 800-50).* p. ES-1.

[16] National Institute for Standards and Technology. (2006). *Information Security Handbook: A Guide for Managers Recommendations of the National Institute of Standards and Technology (NIST SP 800-100)*.

[17] Ibid. pp. 41 – 93.

[18] National Advisory Council Infrastructure. (2006). *Workforce Preparation Education and Research Working Group Final Report and Recommendations by the Council.* pp. 20, 34.

[19] President's Information Technology Advisory Committee. (2005). *Cyber Security: A Crisis of Prioritization.* Arlington, VA: National Coordination Office for Information Technology Research and Development. p. 3.

[20]U.S. Department of Homeland Security. (2009). *National Infrastructure Protection* Plan. Washington, D.C. p. 12.

[21] Ibid. p. 85.

[22] Office of Management and Budget. (2007). *Fiscal year 2007 FISMA Report to Congress on Implementation*

of The Federal Information Security Management Act of 2002. Washington, D.C.: Office of Management and Budget. p. 1.

[23] H. R. Rep. No. 2458—52, 107th Cong., 2nd Sess. (2002).

[24] National Science Foundation and U.S. Department of Homeland Security. (2005). *Federal Cyber Service: Scholarship For Service Information For Students*. Retrieved March 6, 2009, from: https://www.sfs.opm.gov/StudentBrochureWeb.pdf

[25] Lawler, James, Li, Zheng, and De Leon, Yvette. (2004). A Study of Security Education in the Era of Cyber-Terrorism. *Journal of College Teaching & Learning, 2*, 5.

[26] Dark, Melissa, Ekstrom, Joseph, and Lunt, Barry. (2006). Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice. *Journal of Information Technology Education, 5*, 4.

[27] Computing Technology Industry Association. (2009). *CompTIA Certifications, IT Education*. Retrieved February 24, 2009, from http://www.comptia.org/about/default.aspx

[28] Center for Strategic and International Studies. (2008 December). *Securing Cyberspace for the 44th Presidency*. Washington, D.C.:Center for Strategic and International Studies. p. 73.

[29] Kamali, Reza, Liles, Samuel, Winer, Charles, Jiang, Keyuan, and Nicolai, Barbara. (2006). A Curriculum Model Based on the SIGITE Guidelines. *Journal of Information Technology Education, 5*.

[30] Maconachy, W.V., et. al. (2001, June). *A Model for Information Assurance: An Integrated Approach.* Paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.

[31] ACM Computer Security Conference, Kennesaw, GA, (2004).

[32] Association for Computing Machinery. (2005). *Computing Curricula: Information Technology*. p. 19.

[33] National Security Agency. (2009, January 15). *Criteria for Measurement CAE/IAE – NSA/CSS.* Retrieved February 13, 2009, from http://www.nsa.gov/ia/academic_outreach/nat_cae/cae_iae_program_criteria.shtml

[34] Association for Computing Machinery, & Institute of Electrical and Electronics Engineers Computer Society. (2008, November). *Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology. p. 76.*

[35] Dark, Melissa, Ekstrom, Joseph, and Lunt, Barry. Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice. *Journal of Information Technology Education, 5*.

[36] Dark, Melissa. (2002). *CERIAS Tech Report 2002-68: Defining a Curriculum Framework in Information Assurance and Security*. Retrieved February 20, 2009, from Purdue University, The Center for Education and Research in Information Assurance and Security Web site: http://www.cerias.org/bookshelf/archive/2002-68.pdf

[37]Elder, Kevin, Strouble, Dennis, Bouvin, Dave. (2004, November). *Information Assurance Education and the IS Curriculum*. Paper presented at the 21st Annual Conference on Information Systems Education, Newport, RI.

[38] Maconachy, W.V., et. al. (2001, June). *A Model for Information Assurance: An Integrated Approach.* Paper presented at the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.

[39] Petersen, Rodney, Larsen, Ronald, Schou, Corey, Strickland, Lee. (2004). *What's in a Name? The labels associated with security—computer, network, information, information assurance—have multiple implications for higher education*. Retrieved February 20, 2009, from http://net.educause.edu/ir/library/pdf/eqm0430.pdf

Appendix A
Documents Reviewed

Appendix A.1

Document Title	Source	Date
President's Information Technology Advisory Committee Cyber Security: A Crisis of Prioritization	http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf	**February 2005**
FISMA Executive Summary Report	http://www.sec-oig.gov/Reports/AuditsInspections/2008/451final.pdf	**September 2008**
National Infrastructure Protection Plan 2009	http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf	**February 2009**
National Infrastructure Advisory Council Workforce Preparation Education and Research Working Group	http://www.dhs.gov/xlibrary/assets/niac/niac_workforcereport_april06.pdf	**April 2006**
DoD 8570.01M: Information Assurance Workforce Improvement Program Manual	http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf	**December 2005**
DoD Directive 8570.01: Information Assurance Training, Certification, and Workforce Management	http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf	**August 2004**
A Study Of Security Education In The Era Of Cyber-Terrorism	http://www.cluteinstitute-onlinejournals.com/PDFs/2005111.pdf	**October 2005**
Integrating Information Assurance and Security into IT Education: A Look at the Model Curriculum and Emerging Practice	https://www.cerias.purdue.edu/assets/pdf/bibtex_archive/2007-90.pdf	**2006**
Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002	http://georgewbush-whitehouse.archives.gov/omb/inforeg/reports/2007_fisma_report.pdf	**2008**
2008 Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence **National Association of State Chief Information Officers:**	http://www.fbiic.gov/public/2008/feb/Annual_threat_assessment.pdf http://www.nascio.org/publications/documents/NASCIO-InsiderSecurityThreats.pdf	**February 2008** **April 2007**

Insider Security Threats: State CIOs Take Action Now!	http://www.acm.org/education/curric_vols/IT_October_2005.pdf	**October 2005**
Association for Computing Machinery: Computing Curricula Information Technology		
CERIAS Tech Report 2004-116: Integration of information assurance and security into the IT2005 model curriculum	http://www.cerias.purdue.edu/assets/pdf/bibtext_archive/2004-116.pdf	**2005**
ACM & IEEE: Information Technology 2008 Curriculum Guidelines for Undergraduate Degree Programs in Information Technology	http://www.acm.org/education/education/curricula/IT2008%20Curriculum.pdf	**November 2008**

Appendix A.2

Document Title	Source	Date
CNSS Directive No. 500: Information Assurance (IA) Education, Training, and Awareness	http://www.cnss.gov/Assets/pdf/CNSSD_500.pdf	**August 2006**
NSTISSI No. 1000: National Information Assurance Certification and Accreditation Process (NIACAP)	http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf	**April 2000**
CNSS Instruction No. 4009: National Information Assurance (IA) Glossary	http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf	**June 2006**
CNSS Instruction No. 4012: National Information Assurance Training Standard For Senior System Managers	http://www.cnss.gov/Assets/pdf/cnssi_4012.pdf	**June 2004**
CNSS Instruction 4013: National Information Assurance Training Standard For System Administrators (SA)	http://www.cnss.gov/Assets/pdf/cnssi_4013.pdf	**March 2004**
CNSS Instruction 4014: National Information Assurance Training Standard For Information Systems	http://www.cnss.gov/Assets/pdf/cnssi_4014.pdf	**April 2004**

Security Officers		
CNSS Instruction No. 4016: National Information Assurance Training Standard For Risk Analysts	http://www.cnss.gov/Assets/pdf/CNSSI-4016.PDF	**November 2005**

Appendix A.3

Document Title	Source	Date
GAO-08-212T: Internet Infrastructure Challenges in Developing a Public/Private Recovery Plan	http://www.gao.gov/new.items/d08212t.pdf	**October 2007**
GAO-05-827T: Critical Infrastructure Protection Challenges in Addressing Cybersecurity	http://www.gao.gov/new.items/d05827t.pdf	**July 2005**
GAO-06-1087T : Critical Infrastructure Protection DHS Leadership Needed to Enhance Cybersecurity	http://www.gao.gov/new.items/d061087t.pdf	**September 2006**
GAO-07-751T: Information Security Persistent Weaknesses Highlight Need for Further Improvement	http://www.gao.gov/new.items/d07751t.pdf	**April 2007**
GAO-08-1075R: Federal Legal Requirements for Critical Infrastructure IT Security	http://www.gao.gov/new.items/d081075r.pdf	**September 2008**
GAO-08-825: Critical Infrastructure Protection DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise	http://www.gao.gov/new.items/d08825.pdf	**September 2008**
GAO-08-588: Cyber Analysis and Warning DHS Faces Challenges in Establishing a Comprehensive National Capability	http://www.gao.gov/new.items/d08588.pdf	**July 2008**

Appendix A.4

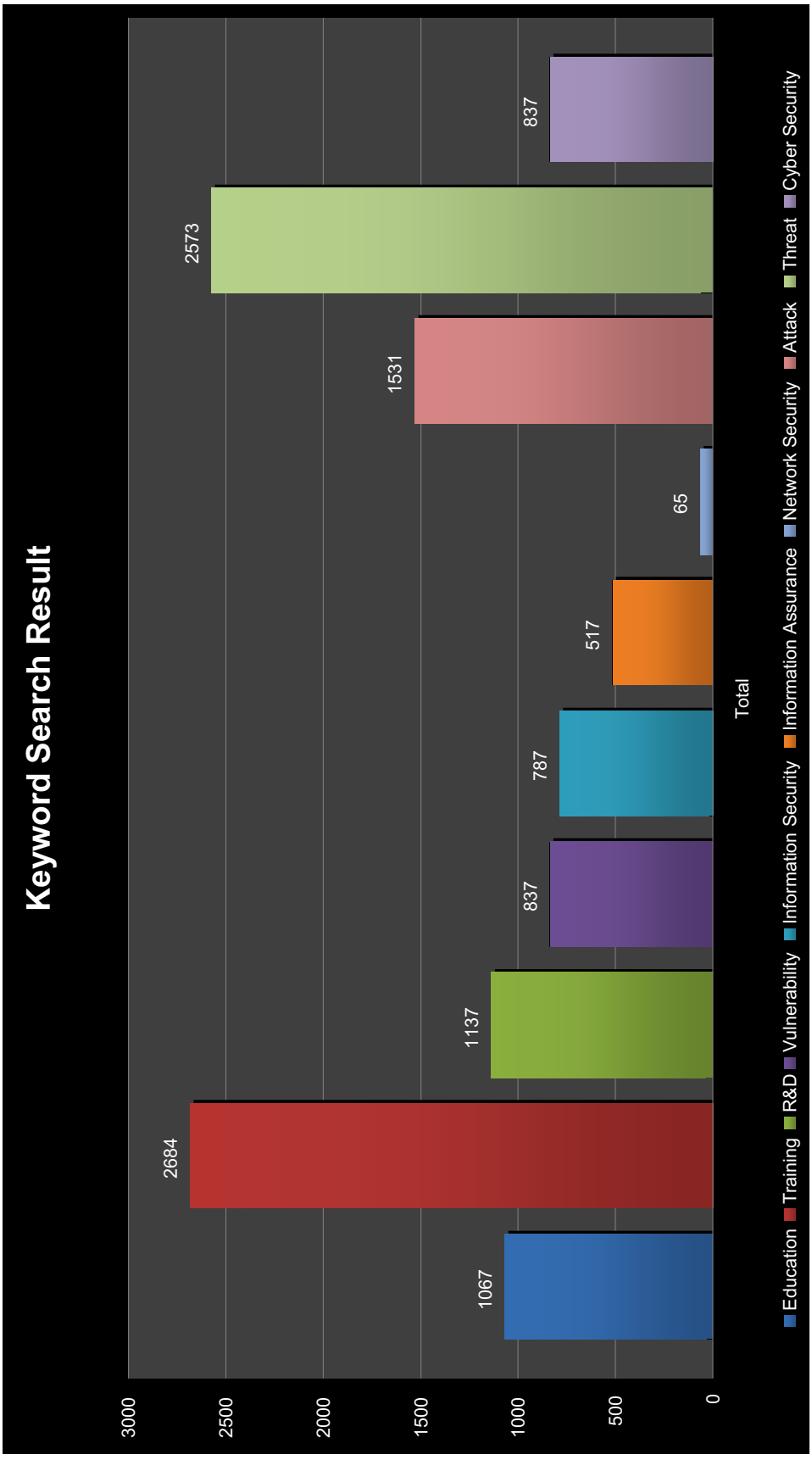
Document Title	Source	Date
Department of Homeland Security Agriculture and Food Sector-Specific Plan	http://www.dhs.gov/xlibrary/assets/nipp-ssp-ag-food.pdf	**May 2007**
Department of Homeland Security Banking and Finance Sector-Specific Plan	http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf	**May 2007**
Department of Homeland	http://www.dhs.gov/xlibrary/assets/nipp-ssp-	**May 2007**

Security Communications Sector-Specific Plan	communications.pdf	
Department of Homeland Security Defense Industrial Base Sector-Specific Plan	http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf	**May 2007**
Department of Homeland Security Energy Sector-Specific Plan	http://www.dhs.gov/xlibrary/assets/nipp-ssp-energy-redacted.pdf	**May 2007**
Department of Homeland Security Information Technology Sector-Specific Plan	http://www.dhs.gov/xlibrary/assets/nipp-ssp-information-tech.pdf	**May 2007**
Department of Homeland Security National Monuments and Icons Sector-Specific Plan	http://www.dhs.gov/xlibrary/assets/nipp-ssp-national-monuments-icons.pdf	**May 2007**
Department of Homeland Security Transportation Systems Sector-Specific Plan	http://www.dhs.gov/xlibrary/assets/nipp-ssp-transportation.pdf	**May 2007**
Department of Homeland Security Water Sector-Specific Plan	http://www.dhs.gov/xlibrary/assets/nipp-ssp-water.pdf	**May 2007**
Department of Homeland Security Information Technology (IT) Security Essential Body of Knowledge (EBK)	http://www.us-cert.gov/ITSecurityEBK/EBK2008.pdf	**September 2008**

Appendix A.5

Document Title	Source	Date
NIST Special Publication 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model	http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf	**April 1998**
NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program	http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf	**October 2003**
NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers	http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf	**October 2006**

Appendix B
Results of Keyword Search



Appendix C
DoD Baseline IA Certifications
As found in *DoD Information Assurance Workforce Improvement Program* (DoD 8570.01-M. May 15, 2008)

JOB See Document for Job Descriptions	REQUIRED CERTIFICATIONS			
TECH I	A+	Network+	SSCP	
TECH II	GSEC†	Security+†	SSCP	SCNP
TECH III	GSE†	CISSP†*	SCNA	CISA†
MGMT I	GSLC†	GSIF†	Security+ †	
MGMT II	GSLC†	CISSP†	CISM	
MGMT III	GSLC†	CISSP†*	CISM	
CND ANALYST	GCIA†			
CND INFRASTRUCTURE SUPPORT	SSCP			
CND INCIDENT RESPONDER	GCIH†	CSIH		
CND AUDITOR	GSNA†	CISA†		
CN-SP MANAGER	CISSP-ISSMP	CISM		
IASAE I	CISSP†*			
IASAE II	CISSP†*			
IASAE III	CISSP-ISSEP†	CISSP-ISSAP		

† SANS TRAINING COURSES AVAILABLE FOR CERTIFICATION
* ASSOCIATE OF CISSP ALSO ACCEPTABLE

CISA - Certified Information Systems Auditor
CISM - Certified Information Security Manager®
CISSP - Certified Information Systems Security Professional
CISSP-ISSAP - Certified Information Systems Security Architecture Professional
CISSP-ISSEP - Certified Information Systems Security Engineering Professional
CISSP-ISSMP - Certified Information Systems Security Management Professional
CSIH - Computer Security Incident Handler
GCIA - GIAC Certified Intrusion Analyst
GCIH - GIAC Certified Incident Handler
GSE - GIAC Security Expert
GSEC - GIAC Security Essentials Certification
GSIF - GIAC Information Security Fundamentals
GSLC - GIAC Security Leadership Certification
GSNA - GIAC Systems and Network Auditor
SCNA - Sun Certified Network Administrator
SCNP - Security Certified Network Professional
SSCP - Systems Security Certified Practitioner