An Exploration of the Current State of Information Assurance Education

Stephen Cooper, Leader
Purdue University
305 University Street
West Lafayette, IN 47907
1.765.494.7505
coopers@acm.org

Christine Nickell, co-Leader
Department of Defense
9800 Savage Road Suite 6722
Ft. Meade, MD 20755
1.410.854.6206
c.nicke2@radium.ncsc.mil

Victor Piotrowski
National Science Foundation
4201 Wilson Blvd.
Arlington, VA 22230
1.703.292.5141
vpiotrow@nsf.gov

Brenda Oldfield
Department of Homeland Security
NCSD
Washington DC 20528
1.703.235.5184
Brenda.Oldfield@dhs.gov

Ali Abdallah
London South Bank University
102 Burrough Rd
London SE1 0AA England
44.20.7815.7027
a.abdallah@lsbu.ac.uk

Matt Bishop
University of California, Davis
One Shields Ave
Davis, CA 95616
1.530.752.8060
bishop@cs.ucdavis.edu

Bill Caelli
Queensland University of Tech.
GPO Box 2434
Brisbane Qld 4001 Australia
61.7.3138.9451
w.caelli@qut.edu.au

Melissa Dark
Purdue University
305 University Street
West Lafayette, IN 47907
1.765.494.5010
dark@purdue.edu

E K Hawthorne
Union County College
1033 Springfield Ave
Cranford, NJ 07016
1.908.497.4232
ehawthorne@acm.org

Lance Hoffman
Computer Science Department
George Washington University
Washington, DC 20052
1.202.994.4955
lanceh@gwu.edu

Lance C. Pérez
University of Nebraska, Lincoln
209N SEC
Lincoln, NE 68588
1.402.472.6258
lperez@unl.edu

Charles Pfleeger
Pfleeger Consulting Group
4519 Daveport St NW
Washington, DC 20016
1.202.680.0540
chuck@pfleeger.com

Richard Raines
Air Force Institute of Technology
2950 Hobson Way, Bldg 642
Wright Patterson AFB, OH 45433
1.937.255.6565 x4278
Richard.raines@afit.edu

Corey Schou
Idaho State University
921 South 8th Ave., Stop 8020
Pocatello, ID 83209
1.208.282.3194
schou@mentor.net

Joel Brynielsson
Royal Inst. of Technology
SE-100 44 Stockholm
Sweden
46.70.5394300
joel@kth.se

ITiCSE'09, July 6-9, 2009, Paris, France.

ABSTRACT

Information Assurance and computer security are serious worldwide concerns of governments, industry, and academia. Computer security is one of the three new focal areas of the ACM/IEEE's Computer Science Curriculum update in 2008. This ACM/IEEE report describes, as the first of its three recent trends, "the emergence of security as a major area of concern."

The importance of Information Assurance and Information Assurance education is not limited to the United States. Other nations, including the United Kingdom, Australia, New Zealand,

Canada, and other members from NATO countries and the EU, have inquired as to how they may be able to establish Information Assurance education programs in their own country.

The goal of this document is to explore the space of various existing Information Assurance educational standards and guidelines, and how they may serve as a basis for helping to define the field of Information Assurance. It was necessary for this working group to study what has been done for other areas of computing. For example, computer science (CS 2008 and associate-degree CS 2009), information technology (IT 2008), and software engineering (SE 2004), all have available curricular guidelines.

In its exploration of existing government, industry, and academic Information Assurance guidelines and standards, as well as in its discovery of what guidance is being provided for other areas of computing, the working group has developed this paper as a foundation, or a starting point, for creating an appropriate set of guidelines for Information Assurance education. In researching the space of existing guidelines and standards, several challenges and opportunities to Information Assurance education were discovered. These are briefly described and discussed, and some next steps suggested.

Categories and Subject Descriptors
K.3.2 Computer and Information Science Education

General Terms
Security.

Keywords
Information Assurance, IA, Education, Standards, Guidelines.

1. INTRODUCTION
Several years ago, there were few faculty members within the undergraduate computing community who were concerned about Information Assurance (IA) or computer security education. It is amazing how much has changed in the world over the past ten or so years. Computer security is now taken quite seriously, internationally, by governments, industry, and academia. One of the three new focal areas of the ACM/IEEE's Computer Science Curriculum update in 2008 [3] is computer security. This report describes, as the first of its three recent trends, "the emergence of security as a major area of concern."

Within the United States (US) government, the primary means for an academic institution to demonstrate the quality of its IA program is through application for and receipt of the National Security Agency (NSA) and Department of Homeland Security (DHS) designation as a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) and/or Research (CAE-R) [13].

What is IA? IA is set of technical and managerial controls designed to ensure the confidentiality, possession of control, integrity, authenticity, availability, and utility of information and information systems. IA includes measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IA is of both national and international significance because of the increased reliance of governmental, military, and financial functions on complex interconnected computer systems and networks. These systems not only store information, they exchange and process information and are involved in increasingly significant decision processes that demand all aspects of information assurance. Society has reaped significant benefits from these systems. With this increased reliance on electronic infrastructure, however, has come the realization that these systems are vulnerable to a myriad of attacks, many of them cyber in nature and not requiring the resources of a world power. This combination of a desire to continue to gain the benefits of complex electronics systems with the recognition of their inherent vulnerabilities has made IA a global priority.

The importance of IA and IA education is not limited to the US or to US institutions. Other nations, including the United Kingdom, Australia, New Zealand, Canada, and other members from NATO countries and the EU, have inquired as to how they may be able to establish a National IA Education program in their own country.

In order to receive a CAE/IAE designation, there is a requirement for US academic institutions to map their IA curriculum to meet the Committee on National Security Systems (CNSS) standard CNSS 4011, as well as one or more of the standards 4012, 4013, 4014, 4015, or 4016 [17]. The use of IA standards for curriculum mapping has been used as a tool to ensure individuals gain or have an understanding of the fundamental IA and security elements. Concerns have developed among many academic institutions over the requirement of mapping curricula to the US government CNSS standards. Many believe these are not sufficiently relevant for current IA education, as they are more training centric and not consistent with the broader education missions of colleges and universities. There are also concerns about relying only on US government based standards, rather than creating an IA curriculum that is internationally relevant.

During the 2009 SFS Symposium in Washington, DC and, simultaneously, during HICSS-42 in Waikoloa, HI, representatives from the government, academia and industry discussed the need for establishing a working group to discuss IA education. In a subsequent meeting, representatives from the NSA, DHS and NSF decided to move forward with a working group effort and to use ITiCSE as a preferred forum due to its international reach and SIGCSE connections. It was noted that in addition to the CNSS standards, there are many other proposed standards and guidelines, including the National Institute of Standards and Technology (NIST) Information Technology Security Training Requirements (publication 800-16, available from [18]), the Department of Defense (DoD) Information Assurance Workforce Improvement Program (DoD Directive 8570, available from [19]), the Department of Homeland Security's Essential Body of Knowledge (EBK), available from [20], and the joint American National Standards Institute (ANSI), International Organization for Standardization (ISO), and International Electrotechnical Commission (IEC) ANSI/ISO/IEC 17024:2003 standard [21].

IA has been addressed as part of broader curricular recommendations. For example, computer science (CS 2008), computer engineering (CE 2004), information technology (IT 2008), and software engineering (SE 2004) all have available

curricular guidelines [11]. These ACM/IEEE reports define bodies of knowledge, suggest specific courses and their content, and describe topic areas and student learning objectives. One limitation of using these reports as a model is that they do not include recommendations for Master's programs (as they focus instead only on undergraduate programs).

IA education has also been addressed through industry. There are several industry-based certifications, and associated guidelines with respect to the content in which these certifications aim to demonstrate knowledge.

This paper starts with the presentation of a brief history of IA Education. It then continues by exploring the existing potential guidance provided by academic, government, and industry standards and guidelines. The paper then explores the area of assessment, before discussing some existing challenges, and concluding. In its exploration of existing IA standards and guidelines, as well as in its discovery of what guidance is being provided from other areas of computing, this paper provides a starting point for creating an appropriate set of guidelines (and a mechanism for enabling future updating to such a set) for IA education.

2. HISTORY OF IA EDUCATION

There is a significant history leading to the emergence of IA as a field unto itself, the roots of which date back to early cryptography, leading to telecommunications security and computer security, followed by information security and then to IA. The focus of this section is to address the significant aspects that have shaped IA in education to date.

In the 1970s, there were industrial conferences, such as COMPSEC that tended to focus on industrial clients' training and continuing education needs, such as audit and security management, and that were directed toward people who would now be known as chief security officers, for continuing education. This industrial IA training led to current commercial training programs such as SANS, ISC^2, and ISACA. At the same time some computer suppliers offered specific education and training courses to enable early computer and data network security systems to be properly administered and used.

Also starting in 1970, faculty members at four-year colleges and universities began to develop and teach computer security and related courses; these faculty numbers increased significantly during the 1980s. [40] The faculty members informally met with colleagues with similar interests and through these interactions broadened the course offerings and the body of knowledge. Research conferences and textbooks encouraged the recognition of computer security as a bona fide sub-discipline. By the early 1980s specific information security journals dedicated to the publication of academic research papers emerged. During this period, however, courses were typically individual offerings and computer security education remained largely unstructured and uncoordinated.

Significant changes began to occur in 1987. The National Computer Security Center (NCSC), of the US National Security Agency (NSA) through a contract with the Institute for Defense Analyses, sponsored an invitational workshop that brought together subject matter experts from government, academia and industry to develop six undergraduate curriculum modules for use by computer science professors as adjuncts to their core curricula courses. This was the first effort by the US government with an objective to promote and coordinate computer security education. A second objective for the course modules was for inclusion in the joint ACM/IEEE undergraduate computer science curriculum. While the workshop effort did not achieve the desired result of getting the modules into the joint curriculum, the modules were informally distributed and used extensively throughout the 1990s with the result that elements of computer security were integrated into core computer science courses.

Also in 1987, Royal Holloway College (now part of the University of London) in England began offering a Master of Science program in Information Security. This program was developed in conjunction with an industrial advisory board to ensure that the graduates met the needs of industry for hiring. In 1986 the Queensland Institute of Technology, now the Queensland University of Technology (QUT) in Australia offered a Masters level research degree in computer security. This led to the formation of the Information Security Research Centre, now merged in to the Information Security Institute, in mid-1988.

Another significant event that influenced IA education was the signing of the US Computer Security Act of 1987. This law was enacted to improve the security and privacy of sensitive information in Federal computer systems, to establish minimum security practices for these systems, and mandated contingency plans and required annual training and awareness for system users. It also mandated that the National Security Agency (NSA) and the National Institute for Standards and Technology (NIST) work together to provide awareness, training and education in this area. This led to the development of IA training and education standards and guidelines that not only guided government, but later influenced commercial and academic IA education.

Further outcomes at least indirectly resulting from the Computer Security Act of 1987 were the formation of the Computer Emergency Response Team (CERT) in 1988, the National Security and Telecommunications Information Systems Committee (NSTISSC) in 1992 and the NIST Security Handbook in 1995. The Computer Security Act of 1987, combined with other legislation, policy and directives, brought about the National INFOSEC Education and Training Program (NIETP) in 1990, the Committee on National Systems Security (CNSS), formerly NSTISSC, standards and the National IA Training and Education Center (NIATEC), which is a repository for IA awareness, training and education documents and modules. The NIETP is housed at the NSA, and its purpose is to provide awareness, training and education to academia to reduce the vulnerabilities of our national information infrastructure.

The European Region Action Scheme for the Mobility of University Students (ERASMUS) project was established in 1987 to facilitate exchanges among European universities [23]. It also included parallel relationships with universities in the US. The ERASMUS program evolved and merged with other independent programs to become the SOCRATES EC program in 1994, later known as the Socrates II program. In July 2001 Professor Louise Yngström, Stockholm University, Sweden and Professor Sokratis Katsikas, University of the Aegean, Greece presented a paper at IFIP TC11 WB 11.8 Information Security Education that discussed the interoperability of computer security and IA programs. The program allowed for student and staff exchanges between member institutions and developed a proposal for a postgraduate curriculum on Information & Communication Systems Security. The Erasmus Project and its descendents award

degrees in Information Systems Security and Computer and Communication Systems Security. It has been instrumental in the growth of the IA and computer security fields.

In 1989, the Council of European Professional Informatics Societies (CEPIS) was formed as a non-profit organization to improve and promote a high standard among Informatics Professionals (in the IT professional field) in recognition of the impact that Informatics has on employment, business and society. CEPIS represents 36 Member Societies in 33 countries across greater Europe. CEPIS not only looks to address IT standards, but also addresses education and research matters related to IT practices. An offshoot of this group is the European Union Certification of Informatics Professionals (EUCIP). EUCIP includes partners in 8 countries (Croatia, Estonia, Ireland, Italy, Norway, Poland, Romania, Spain) offering certification of IT competencies in a vendor neutral framework. EUCIP works to define industry IT standards and to close the gap in the labor market. Currently, EUCIP is taking part in a project called "HARMONISE - Review of Certification Schemes for Information and Communications Technology (ICT) Professional qualifications in support of greater Harmonisation across Europe and beyond" to create harmonization across the EU on Information and Communications Technology ICT professional vocational learning and qualification schemes.

In 1991 the International Federation for Information Processing (IFIP) chartered workgroup WG 11.8 of its Technical Committee 11, dedicated to information security, [22] to promote information security education and training at the university level and in government and industry. WG 11.8 is an international resource center for the exchange of information in this education arena and has sponsored a number of relevant international workshops.

During the early 1990s courses and programs continued to expand, for example, COAST (at Purdue University) and CISR (at the Naval Postgraduate School). These programs brought together a critical mass of faculty, research support and students. IA curriculum development efforts were also sponsored by the major professional societies such as ACM, IEEE, the British Computer Society, and the Australian Computer Society. Additional efforts in 1997, such as the first annual first annual ACM and Naval Postgraduate School Workshop on Education in Computer Security and the first annual National Colloquium for Information Systems Security Education, brought about collaboration between the government, academia and industry to effect IA education. In Australia, the Queensland University of Technology started offering a Postgraduate Certificate and Diploma in information security as well as a Masters Degree program by coursework.

In 1998 the Centers of Academic Excellence in Information Assurance Education (CAE/IAE) program was formed by the NSA to recognize institutions with significant IA education programs and encourage other institutions to develop such offerings. The IA courseware evaluation (IACE) program utilized the modified CNSS standards as prerequisite criteria for the CAE program. In 1999 the first seven institutions were designated. The program was intended to advance with technology so member institutions were required to be re-designated every three years. In 2004, as a result of the 2003 "President's National Strategy to Secure Cyberspace", DHS partnered with NSA in the National CAE program. In 2008 the CAE program was expanded to recognize excellence in IT innovation and Research (CAE-R). Combined, there are 106 CAEs with designation of one or both. The CAE programs have shown success by producing graduates with at least a minimum understanding of the IA and information security principles. These CAE graduates have more current IA knowledge and skills that they bring into the workforce, and are highly sought after. Both of these programs assist in reducing the vulnerabilities within industry, government and academia. These graduates can then help fill the void that the upcoming retirement eligible personnel will leave.

In 2001, the US Congress enacted legislation to begin the National Science Foundation (NSF) Scholarship for Service (SFS) program [14], and the Department of Defense (DoD) Information Assurance Scholarship Program (IASP) [15, 16]. This legislation authorized academic institutions with CAE designation to apply for IA scholarship and capacity grants. These programs were formed to create a pipeline of graduates with IA backgrounds for the federal government through a service obligation (payback). The capacity portion of the programs enables development of IA faculty, curriculum, and lab at CAEs and other institutions to increase the overall capacity of IA educated students for American schools.

In 2002 NSF supported a workshop hosted by the American Association of Community Colleges. This workshop was to articulate the purpose of two-year degrees and educational programs in the broader IA context. Their report, entitled "The Role of Community Colleges in Cybersecurity Education," focused on how community college resources could be used and further developed to help educate a cybersecurity workforce.

In 2005 NSF funded (through its Advanced Technological Education program) three regional centers in IA, which are CyberWATCH, Cyber Security Education Consortium (CSEC) and the Center for Systems Security and Information Awareness (CSSIA). These centers are partnerships between two-year institutions, four-year institutions and industry. The purpose of these centers is to provide leadership and training in IA education at two-year institutions.

In 2005 the "Computing Curricula 2005" report, jointly published by ACM and IEEE-CS, was written to provide an overview of the different kinds of undergraduate degree programs in computing that are currently available and for which curriculum guidelines are now, or will soon be, available.

As a consequence of the overall cyber threat and the need to integrate IA efforts into civil security at large, a trend during recent years has been to let large-scale IA exercises affect curricula development and course design. Such large-scale exercises are being undertaken as part of countries' homeland security efforts and, most often, universities and university teachers are involved in the actual execution of these exercises. As an example, the annual "cyber defense exercise" in the US is sponsored by the NSA and involves a number of schools related to civil security. In this exercise, the participating schools are to learn defensive IA by designing and implementing a network that provides certain services and defending this network from both natural events and the cyber attacks that are initiated by the "red force" of hackers from the NSA. This exercise helped shaping the IA curriculum and course format at the Air Force Institute of Technology [37].

In the EU, the cyber attacks on Estonia and Georgia have served as a starting point for multinational exercises involving various governmental organizations. A recent example of this engagement

occurred in December 2008 when Sweden and Estonia came together in a joint cyber defense exercise. In cooperation with the Cooperative Cyber Defence Centre of Excellence in Estonia, the exercise was sponsored by the Swedish Civil Contingencies Agency and run jointly by a number of Swedish authorities: the Defence Research Agency, the National Defence Radio Establishment (FRA), the National Defence College, and the Defence Materiel Administration. Similar to the aforementioned "cyber defense exercise" in the US, CS students from the universities in Tallinn (Estonia) and Linköping (Sweden) acted blue teams while being under attack by the FRA (roughly, FRA is the Swedish equivalent of the NSA).

The most important reason to let large-scale exercises shape curricula or course design is to let students obtain a working knowledge in actually using their skills to interact with the society at large, i.e., to see the overall picture and to perform under pressure in critical situations. However, using large-scale homeland security IA initiatives as a foundation for shaping university curricula raises concerns with regard to being too training centric and not consistent with the scholarly mission of colleges and universities. See Section 1 where similar concerns are discussed with regard to using IA standards for curriculum mapping.

3. GUIDANCE

3.1 Academic Guidelines

In this section, guidelines for accrediting academic programs are discussed starting with the Computing Curricula 2005 Overview Report as it sets the context for the individual guidelines. In turn, each guideline is presented, focusing on: 1) an executive summary, 2) creating the guideline, 3) updating the guideline, 4) instructional recommendations, and 5) Information Assurance and computer security knowledge.

3.1.1 ACM/IEEE Computing Curricula 2005: the Overview Report

Executive Summary

The primary purpose of the Computing Curricula 2005 report is to "provide an overview of the different kinds of undergraduate degree programs in computing that are currently available and for which curriculum standards are now, or will be soon, available" [1]. The overview report identifies the different computing-related degree programs and distinguishes their similarities and respective differences. As stated in the introduction, the report is intended for use by a variety of stakeholders, including university faculty and administrators with existing and planned computing programs, stakeholders in public education, students and prospective students trying to decide upon a major, parents and guidance counselors who assist in such decisions, and professionals working in the dynamic and rapidly changing computing fields. The overview report focuses on comparison and contrast of five computing degree programs: computer engineering (CE), computer science (CS), information systems (IS), software engineering (SE), and information technology (IT). The respective programs are compared to each other on two dimensions: relative amount of theory vs. application and five areas of knowledge. The report then provides considerable detail via a numerical rating of relative emphasis on 40 computing topics and 17 non-computing topics.

Creating the Guideline

In the late 1980s, ACM and IEEE collaborated to produce a joint curriculum report for computing, which was published in 1991. Given the dramatic growth in computing, the need to update and expand this report was apparent by the late 1990s. Again, these two societies joined forces to address this need and provided financial support as well as intellectual leadership. A task force was assembled, only this time the Joint Task Force included individuals from additional professional associations such as the Association for Information Systems and Association for IT Professionals, in recognition of the growing diversity and breadth of computing. Each of the respective professional societies was charged to undertake a cooperative effort to create the respective disciplinary volumes. This report provides context for the other disciplinary curricula guidelines and was derived in large part from the detailed information provided in those guidelines.

Updating the Guideline

There is no specific mention of a proposed mechanism for updating the Computing Curricula 2005 – The Overview Report. However, clear steps are outlined with regard to updating each of the respective discipline-specific guideline. The Joint Task Force recommends that the Computing Curricula Series be updated every 5 - 6 years, given the rapid pace of change in computing.

Instructional Recommendations

Two contrasting curricular structures are discussed in the Overview Report: filter and funnel. The filter approach essentially treats each computing field as distinct, thereby necessitating discipline-specific introductory courses sequences: the funnel approach provides for a common introductory sequence and then "funnels" students into disciplinary tracks. Interested readers are directed to the original report for further discussion of the pros and cons of each approach.

Information Assurance and Computer Security Knowledge

The Overview Report explicitly mentions in Table 3.1 *Comparative weight of computing topics across the five kinds of degree programs* ([1], p. 24) IA and computer security topics under two knowledge areas: security, issues and principles; security, implementation and management. Table 3.1 also lists the legal, professional, ethics, and society knowledge area that is conceivably a related topic to IA and computer security. In Table 3.2 *Comparative weight of non-computing topics across the five kinds of degree programs* ([1], p. 25) is another possible related topic entitled risk management/project safety.

3.1.2 ACM/IEEE Information Technology 2008

Executive Summary

The IT 2008 discipline specific report includes recommendations for four-year undergraduate programs in information technology. The IT body of knowledge is organized into 13 knowledge areas: IT Technology Fundamentals, Human Computer Interaction, Information Assurance and Security, Information Management, Integrative Programming & Technologies, Math and Statistics for IT, Networking, Programming Fundamentals, Platform Technologies, Systems Administration & Maintenance, System Integration and Architecture, Social and Professional Issues, and Web Systems and Technologies.

Each knowledge area is further defined by units, and units are further defined by topics. The report contains learning outcomes and advanced IT outcomes for each topic in the IT body of knowledge.

Creating the Guideline

Creation of IT2008 commenced in 2001, with informal meetings among faculty members at a small number of institutions. In December, 2001, the first Conference on Information Technology Curriculum (CITC-1) was held. At CITC-1, work began on a list of topics and subtopics, while concurrently building a parent organization (SITE – the Society for Information Technology Education). From 2001-2003, work on the draft continued, using input collected via focus groups from conferences and industrial advisory boards. Draft 1 criteria were posted in 2003 followed by a public review and comment period. Modifications were made using this input. A second draft of the Overview Report became available in 2005 and using this input, the IT draft was updated and posted on the ACM website for another round of public comment. In 2007, a steering committee was formed to guide completion of the document. Using the input from the second round of public comment and the newly formed steering committee, the IT guideline was updated again, made available for public review, and ultimately finalized in November 2008.

Updating the Guideline

There is no explicit mechanism for updating this guideline.

Instructional Recommendations

The IT 2008 Curriculum Guidelines specifically note that four-year IT programs need to be designed so that students develop a practical understanding of technology. While particular delivery mechanisms are not advocated, the guideline suggests that there should be a considerable experiential learning aspect for the IT student. Mechanisms for integrating experiential learning are provided by way of example, such as demonstrations, labs, field trips, project-based learning, internships and co-ops. The IT 2008 report notes that the focus on experiential learning is not intended to suggest that theoretical knowledge is not/should not be taught in an IT program; rather, the point is that a graduate from a four-year IT program must both understand the theory behind the technology and be able to apply the technology in a practical sense to the needs of the organization.

Information Assurance and Computer Security Knowledge

The IT 2008 guideline dedicates a knowledge area just for IA and computer security topics entitled "Information Assurance and Security."

IA and computer security topics also appear in this guideline in three other ways: 1) as a unit within other knowledge areas, 2) as a pervasive theme throughout all knowledge areas, and 3) as an area for advanced courses [2]. The reader is advised to consult the full curriculum guideline for further details.

3.1.3 ACM/IEEE Computer Science 2008 (An Interim revision of CC2001)

Executive Summary

This revision of the CC2001 curriculum [5] was guided by several principles, divided into three groups. The principles of computing emphasize the breadth of computing, including the need for the curriculum to be international in scope, informed by professional practice, and attractive to potential students. The principles on computer science focus on the breadth of the subject's foundations, as well as the focus on underlying concepts and the need to not bind what is taught to existing technology. The principles on course design and implementation suggest that the curriculum should include strategies and tactics for teaching, along with high-level recommendations, and should also provide guidance on the design of individual courses.

Creating the Guideline

Recognizing that the CS2001 volume needed to be updated, the ACM Education Board and the IEEE Computer Society Education Activities Board commissioned a Review Task Force. The mandate included consulting with the academic community and industry. This consultation involved creating a web site for comments, sending e-mails inviting comments, holding public meetings, and talking to people at other meetings and individually. Finally, fifteen participants including representatives of ACM, IEEE Computer Society, industry, and two-year colleges discussed the work with the Review Task Force.

Updating the Guideline

The CS2008 volume expresses the need to update the curriculum on an ongoing basis, so that individual components can be updated as needed. The ACM and IEEE Computer Society have formed a joint group to do this.

Instructional Recommendations

The recommendations are organized into core units and elective units. Core units are "those units required of all students in all computer science degree programs" ([3], p. 26). In general, CS2008 avoids discussing how courses are to be structured; instead specifying what material is core and thus needs to be covered. But, owing to the need to inject security-related material (traditionally seen as an advanced topic) into the core material, CS2008 includes guidance for a basic course in computer security.

Information Assurance and Computer Security Knowledge

CS2008's coverage on IA and computer security in the section Programming Fundamentals includes Foundations of Information Security (4 hours), at an applied level (security goals, standards, and policies; defense in depth; common threats) and Secure Programming (2 hours), again at an applied level (avoiding array and string overflows, and smashing the run-time stack). The learning objectives are tightly tied to these topics.

An elective unit in Risk Assessment expands on some topics in the Foundations of Information Security. This unit amplifies the analysis of risk, including basic concepts, the need for a holistic analysis and risk assessment, principles, and cost/benefit analysis. The learning objectives include applying the unit content to several simple scenarios, including one involving security.

An elective unit in Robust and Security-Enhanced Programming expands on the topics in the Secure Programming core course. This unit covers principles of defensive programming (for example, least privilege and fail-safe defaults) and documenting security considerations when programming. It also covers the "principle of psychological acceptability." Learning objectives also expand on these topics.

CS2008 describes an elective unit in Cryptographic Algorithms, with the topics including private and public key cryptography and key exchange, as well as digital signatures and security protocols. The learning objectives are basic: describe number-theoretic algorithms related to public key cryptosystems, and at least one public key cryptosystem, as well as creating simple extensions to cryptographic protocols.

The section on Societal and Professional Issues has several security-related units, including core units of Privacy and Civil Liberties, Professional Ethics, Risks, and elective units on Security Operations and Computer Crime. So does the section on Human-Computer Interaction, specifically a unit on Human Factors and Security with topics of security policies and psychology, usability and security, and identity theft and phishing. The Programming Languages section's unit on Virtual Machines covers their use as security mechanisms, and security enters into several units in Net Centric Computing, notably the Network Security, Networked Applications, and Network Management units. The latter units emphasize both theory and practice (monitoring networks, gathering and analyzing network traffic).

The Operating Systems section includes a unit on Security and Protection, with topics covering IA in operating systems, including patching, backups, and the separation of policy and mechanism.

Other units contain some elements of IA and security. For example, the core unit on Software Project Management has a topic on risk analysis; a unit on Software Verification and Validation includes topics of testing, validation, verification, and reviews and auditing; a unit on Information Modes includes a topic on information privacy, security, and integrity.

An appendix in this guideline [3] describes an introductory course in computer security. This course parallels many being taught now. It discusses theoretical issues, standards, principles, systems (including host-based access controls and networking fundamentals), operations, attacks and defenses, forensics, and ethics. This outline is presented to provide guidance in creating such a course because of "areas of concern in the curriculum and changes in emphasis since CS2001."

3.1.4 ACM/IEEE Software Engineering 2004

Executive Summary

The SE 2004 curriculum guideline [4] includes recommendations for software engineering programs by identifying the SE core knowledge areas and associated units and topics for each knowledge area. Core refers to material that should be included in any SE program and is not a complete curriculum. The Guideline also includes the amount of time required to cover each unit. This architecture (knowledge area, unit and topic) is consistent with the structure of IT 2008 and CS 2008 (the Interim Revision), as is the utilization of a recommended amount of time. However, the SE 2004 includes two additional recommendations: 1) a knowledge level that each graduate should possess, and 2) the relevance of the topic to the core. The three knowledge levels, based on Bloom's taxonomy, are knowledge (K), comprehension (C), and application (A). The three degrees of relevance are essential (E), desirable (D), and optional (O).

Creating the Guideline

The SE 2004 guideline was developed in three phases with the input of a Steering Committee and a number of other volunteers. Phase one commenced in spring 2002 and included identification of an initial set of knowledge areas. Through public review and comment, this was refined and finalized in March 2003. In October 2002 another group began working on pedagogy guidelines and curriculum models using the *draft* knowledge areas that the first group produced. These guidelines were refined by the Steering Committee as the knowledge areas were evolved. Both pieces were then merged into a draft guideline and augmented with additional material to construct a full draft available for public review and comment beginning July through September 2003. Using this feedback, this guideline was revised and published in 2004.

Updating the Guideline

There is no explicit mechanism for updating this guideline

Instructional Recommendations

The SE 2004 guideline provides 19 curriculum design and delivery guidelines that serve to inform *how* the SE body of knowledge should be taught. This guideline calls for the curriculum to develop students' general thinking skills, e.g., critical judgment and problem solving abilities, as well as their personal skills such as teamwork and communication. Also this guideline recommends the use of active learning strategies such as project-based classes, case studies, problem-based learning, just in time learning, and learning by failure as these instructional strategies have been shown to promote the development of these desired learning outcomes.

Information Assurance and Computer Security Knowledge

IAS can be found explicitly mentioned throughout the SE 2004 Curriculum Guideline as a topic embedded with various units, which are in knowledge areas. For example, in the knowledge area entitled Mathematical and Engineering Fundamentals and the unit on Engineering Foundations for Software, one of the topic areas is systems development (e.g., security, safety, performance, effects of scaling, feature interaction, etc.). This topic is listed at the knowledge level in Bloom's taxonomy and as essential in terms of relevance to the SE core.

A second example is in the knowledge area entitled Software Modeling and Analysis and the unit entitled Analysis Fundamentals. The IAS relevant topic is listed as analyzing quality (non-functional requirements) (e.g. safety, security, usability, performance, root-cause analysis, etc.). This topic is listed at the application level in Bloom's taxonomy and as essential in terms of the relevance to the SE core. Another IAS related topic listed with this unit and knowledge area is prioritization, trade-off analysis, risk analysis, and impact analysis, which is at the comprehension level of Bloom's taxonomy and essential to the SE core.

3.1.5 Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software (SwA CBK)

Executive Summary

Targeting educators as well as trainers, the document focuses on the production of secure software. In the describing the audience for this document, the introduction states: "Educators and trainers wishing to develop specific curricula and curricular material will benefit from this comprehensive summation of the topics, facts, principles, and practices of software-specific security and its assurance. This represents a body of knowledge (BOK) that can provide a benchmark for educators and trainers. This benchmark will enable them to target and validate detailed learning objectives, develop coherent instructional plans, and structure their teaching and evaluation processes to effectively teach specific content across the wide range of relevant audiences and roles." The focus is on the security properties for software (confidentiality, integrity, availability, accountability, and non-repudiation) and the knowledge needed to engineer secure software (threats, vulnerabilities, attacks, etc).

Creating the Guideline

In 2003, the US Department of Defense (DoD) launched a Software Assurance Initiative. The Department of Homeland Security (DHS) joined in this initiative in 2004. The DoD and DHS Software Assurance initiatives have submitted internal, interim reports and held jointly sponsored Software Assurance Forums and a number of individual working group (WG) meetings. A working group was created to focus on workforce education and training. The working group was tasked with responding to the following two questions: "What are the engineering activities or aspects of activities that are relevant to achieving secure software? What knowledge is needed to perform these activities or aspects? " [6] Influenced by the efforts of the software engineering SWEBOK [7] efforts, as well as by the Committee on National Security Systems (CNSS) Training Standards 4011 and 4012 standards, the working group went through several revisions with public comment periods to produce this final guideline.

Updating the Guideline

The acknowledgements section states: "The Working Group's life extends beyond the production of this guide, and its goals remain the same, to help create a workforce capable of developing, sustaining, assuring, and acquiring (more) secure software – but its specific activities may vary. The Working Group welcomes participation in its ongoing activities." [6] However, no specific means of updating this body of knowledge are described in detail.

Instructional Recommendations

There are no specific instructional recommendations per se. Information is not presented as objectives and student outcomes. Rather the focus is on providing the information, and the instructor is expected to merge the material into the course content, to meld with the existing student learning outcomes. In many ways, the document reads as a textbook, describing the different aspects of security throughout the software development life cycle. Additionally, a comprehensive bibliography is provided for each topic area.

Information Assurance and Computer Security Knowledge

IA and computer security topics covered in this guideline include: 1) Threats and Hazards, 2) Fundamental Concepts and Principles, 3) Ethics, Law, and Governance, 4) Requirements, 5) Software Design, 6) Software Construction, 7) Verification, Validation, and Evaluation, 8) Tools and Methods, 9) Process, 10) Management, 11) Sustainment , and 12) Acquisition. Note that while many of these topics occur in any software engineering course, the focus of each topic is on how security relates to and is involved in that topic.

3.1.6 Australian Computer Society CORE Body of Knowledge for Information Technology Professionals

Executive Summary

The "CORE Body of Knowledge for Information Technology Professionals" [8] was developed with the following rationale (from its Preamble): "Information technology professionals are increasingly responsible for the incorporation of security services and mechanisms into overall information systems under development and in operation. This responsibility is expected to increase as national and international Guidelines and legislation are developed and enforced. The I.T. Professional will need to be familiar with Social, Governmental and Legal requirements in this area and to incorporate appropriate technologies into systems during the development phase with appropriate levels of security management created for ongoing usage of the systems." The general topic areas include: Computer Organization and Architecture, Conceptual Modeling, Database Management, Data Communications and Networks, Data Structures and Algorithms, Discrete Mathematics, Ethics/Social Implications/professional Practice, Interpersonal Communications, Program Design and Implementation, Project Management and Quality Assurance, Security, Software Engineering and Methodologies, Systems Analysis and Design, and Systems Software.

Creating the Guideline

Until the 1990s, curricula for undergraduate computing programs in Australia had been developed by overseas professional associations such as ICCP, BCS, ACM and DPMA and typically adopted and recommended by the ACS in the design of tertiary computing courses in Australia.

In Australia in November 1992, the ACS published a report entitled "The ACS Towards 2000." One of the terms of reference emerging from the study was to "determine the common body of knowledge appropriate to the overall discipline of Information Technology" ([9] p.2).

The "CORE Body of Knowledge for Information Technology Professionals" was approved by the Council of the Australian Computer Society in September 1997.

Updating the Guideline

There is no explicit mechanism for updating this guideline.

Instructional Recommendations

The document indicates that the quantity of material "exceeds what could be reasonably covered in any undergraduate IT [program]." No explicit instructions are provided as to the specific material coverage. This BOK specifically avoids providing guidelines for "accreditation of tertiary courses at the professional level." But, it is quite comprehensive in the presentation of content areas in IT.

Information Assurance and Computer Security Knowledge

IA and computer security topics covered in this body of knowledge include: 1) Historical Background, 2) Societal, Governmental and Legal Imperatives for Information Systems Security and Privacy, 3) Professional Responsibility and Information Systems Security, 4) Computer Security, 5) Access control, Authentication, Integrity, Confidentiality, 6) Security Technologies, 7) Key Management, 8) Modes of usage, 9) Network Security, 10) Security services and mechanisms, 11) Computer-telephone integration, 12) Trusted Systems and Networks, 13) Concepts of security functionality and enforcement/verification, 14) Verification techniques and software engineering, 15) Security in the Distributed Systems (Client/Server) and Object Oriented Environments, 16) Security and Specific Industry Requirements, and 17) Security Management.

3.1.7 ACM/IEEE Guideline for Associate-Degree Transfer Curriculum in Computer Science 2009

Executive Summary

Community and technical colleges, as well as certain four-year colleges award associate degrees to students completing two years of postsecondary study. Associate-degree programs are complete in their own right, whether designed specifically to enable graduates to transfer into the upper division of a baccalaureate program or to gain entry into the workforce.

Whether referred to as "computer security", "information security", "Information Assurance" or "software assurance", a curriculum for creating and maintaining secure computing environments is a critical component in associate-degree computing programs.

IA and computer security curriculum can be addressed in a variety of implementation strategies. One approach is to offer a host of individual courses on specific IA and computer security topics. This approach can provide a wealth of content opportunities for specialization, but may create scheduling challenges for many students.

Another approach is to fully integrate and incorporate these fundamental topics into core computing courses with specialized courses reserved for targeted settings; this integrated approach is promoted by the ACM Two-Year College Education Committee.

Creating the Guideline

Recognizing that the CC2001 curriculum [5] needed to be updated, the ACM Education Board and the IEEE Computer Society Education Activities Board commissioned a Review Task Force. The mandate included consulting with the academic community and industry. Finally, fifteen participants including representatives from ACM, IEEE Computer Society, industry, and two-year colleges discussed the work with the Review Task Force.

In conjunction with CS2008, ACM's Two-Year College Education Committee published in January 2009 the *Guideline for Associate-Degree Transfer Curriculum in Computer Science* [10] to foster student matriculation from the lower division into the upper division. This associate-degree guideline was approved by the ACM Education Board and is located online [11].

Updating the Guideline

The CS2008 volume expressed the need to update the curriculum on an ongoing basis, so that individual components are updated as needed. Likewise and in parallel with CS2008 efforts, the ACM Two-Year College Education Committee also updates its associate-degree computer science transfer guideline on a continuous basis via its Curriculum, Assessment, and Pedagogy online environment (CAP-Space) [12].

Instructional Recommendations

It is important to engage students' innate interests early in their academic careers to cement their commitment to computing, to further student retention, and to motivate achievement in their coursework. Faculty at two-year colleges must remain aware of the importance of incorporating professional practices and applied work as an integral part of computing programs. Computing students should be encouraged to: work in teams, use techniques of task and time management, solve practical problems in course projects, make presentations, confront issues of privacy, confidentiality and ethics, use current technology in laboratories, attain real-world experience through cooperative education, internships, and/or other practicum activities, and participate in student chapters of computing societies and organizations.

Information Assurance and Computer Security Knowledge

This guideline advocates strongly for learning activities that require students to actively demonstrate mastery of IA and computer security knowledge, as well as the tenets of professional conduct and ethical behavior in a holistic manner.

The foundation of this curriculum is the three-course computing sequence CS I - CS II - CS III. IA and computer security topics along with their associated learning outcomes are covered in deeper and deeper fashion as a student progresses from CSI to CSII to CS III. In CS I, general topics include secure coding and ethical conduct. More specifically, students use encapsulation, information hiding, and strict data typing to incorporate security into their applications. In CS II, general topics include software assurance, and societal and privacy issues. Students specifically use security-aware exception handling to help prevent buffer overflows, memory leaks, back-door accesses, and malicious code attacks. In CS III, general topics include software and IA as well as professionalism. Specifically, students develop and ensure robust attack-resistant code by testing applications against known software vulnerabilities.

This core sequence is also accompanied by the opportunity for additional computing courses based on a variety of factors, including transfer requirements, institutional specializations, and student interests. One such sample course, Essentials of Computer Security, is described in this guideline.

3.2 Government Standards and Guidelines

This section presents executive summaries of extant government standards and guidelines related to IA education. This includes standards and guidelines developed by individual governments and standards and guidelines developed by international organizations consisting of government members. The historical context, ownership and intended audience, methods for approval and updating, and brief comments about their impact and relationship to IA education are given for each standard or guideline.

3.2.1 ISO 17024:2003

ISO is the International Standards Organization that establishes how systems and products interoperate. One standard they have promulgated is ISO/IEC 17024:2003. It specifies requirements for a body certifying persons against specific requirements, including the development and maintenance of a certification scheme for personnel. [21]

To be certified, the organization must explicitly define the competencies they are intending to certify. They can do this by defining the knowledge, skills and abilities (KSAs) that comprise the discipline. In addition, the standard requires that development of instruction and testing be separate functions and that the examination be evaluated using appropriate psychometric tests for validity.

Certification under ISO 17024:2003 is essential for certifying organizations in the United States if they intend to have their certifications used by the Department of Defense (DoD 8570.m.1, see Section 3.2.4).

None of the provided federal standards or guidelines is intended to be part of the development and maintenance of a certification scheme for personnel. These are designed to provide guidance for the development of training and certification programs for the US government.

3.2.2 NIST SP800-16 1998

NIST Special Publication 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based (Model Revised SP 800-16, Rev. 1 of March 2009). This standard has a common core of KSAs as the CNSS Instructions.

Executive Summary

This document is a "living handbook" and the foundation of and structure for "do-able" training by Federal agencies. By design:

- Dates, references, or other items that would quickly outdate the Training Requirements are excluded as are "terms du jour" and items which may be specific to a given agency or Department. To avoid unnecessary outdating, the document uses terminology that is most consistent across Federal agencies and broadest scope.
- An extensible set of KSAs structure the Training Requirements and are linked to the document through generic IT Security Body of Knowledge new technologies and associated terminology may be added to the KSAs (which are to be maintained in a separate database), and will be tracked forward through the generic IT.

FISMA [39] does not specify role-based training for these individuals. The Office of Personnel Management (OPM) does in their June 2004 mandate – 5 CFR, Part 930. The OPM regulation reinforces FISMA regarding users being exposed to information security awareness, or "awareness training." OPM takes the FISMA requirement for training of those with significant responsibilities for information security a step further, specifying "role-specific training in accordance with NIST standards and guidance." This publication updates what was presented in 1998, and captures these latest federal mandates regarding information security "awareness training" and "role-based training."

What is it? (standard/recommendation/guideline/other) And is it mandatory or optional?

SP 800-16 (and 800-16, Rev. 1) is a NIST guideline. It is offered as a recommendation to federal departments and agencies. A recent OMB dictate made NIST SPs mandatory. OPM's 5CFR Part 930 directs federal organizations to use NIST "standards and guidelines" to develop role-specific training.

Historical context: SP 800-16 was published in April 1998. It was written by members of the Federal Information Systems Security Educators' Association (FISSEA) in the 1990s. It is based on [36]. A draft of the document was passed to NIST in mid-1997. Following editing and a public review and comment period, NIST published it, replacing the previous NIST information security training document 500-172.

Who is the target audience? Who are the stakeholders?

Target audience: Federal information security professionals and instructional design professionals. (Supplemented by CNSS standards for NSI systems) Stakeholders: NIST Computer Security Division (CSD).

Mechanisms/provisions for its update: Who is the owner?

The owner is NIST CSD.

Whose approval is needed?

Approval to update the original document came from NIST CSD management. Approval for the development of the initial document came from an agreement between NIST CSD and the FISSEA Executive Board in the 1993-1994 timeframe.

How often is it updated?

As needed.

Does it conform to the ISO 17024:2003 Personnel Certification Accreditation standard?

Conforming to 17024 is not in the mission of the organization and is not the intent of the document.

What is the value of the standard as it relates to the IA Educational effort/initiative?

If training standards and/or guidelines are perceived to be appropriate tools for the development of college and university course curricula, then this document has value. If training standards and/or guidelines are perceived to be inappropriate tools for the development of college and university course curricula, then this document has less value.

3.2.3 CNSS NSTISSC

These standards have been provided by National Security Telecommunications and Information Systems Security Committee (NSTISSC) as the Committee on National Security Systems (CNSS). They are comprehensive standards for organizations that deal with National Security Information (NSI).

Executive Summary

The CNSS standards have been developed as education and training standards to support the national security infrastructure. CNSS is composed of 21 federal agencies and many observer

organizations from around the federal government. There are currently 6 standards:

- NSTISSCI 4011 IA Professional – Update in progress
- CNSSI 4012 Senior Systems Managers – Updated 2004 -- Update in progress
- CNSSI 4013 System Administrators – Updated 2004 -- Update in progress
- CNSSI 4014 Information System Security Officers – Updated 2004 -- Update in progress
- NSTISSI 4015 System Certifiers – Updated 2005 -- Update in progress
- CNSSI 4016 Risk Analyst – 2008

The standards have been developed using the same eDACUM (electronic Develop a Curriculum) model as the NIST 800-16 documents. This model uses a panel of experts in an electronic decision system. One-half the participants over the years have been from government with the remainder from industry and academia. They are called training standards for consistency with the requirements of PL 100-235. They are maintained in a cross-referenced database and have been scheduled for an update every three years.

What is it? (standard/recommendation/guideline/other) And is it mandatory or optional?

CNSS standards are Instructions/Guidelines for development of training to support National Security Information (NSI) systems for the federal government. They are advisory for management and instructional design. Historically these have been the foundation for emerging academic programs in the US.

Who is the target audience? Who are the stakeholders?

The target audiences are federal agencies charged with maintaining National Security Information (NSI). The stakeholders are the NSI community.

Mechanisms/provisions for its update: Who is the owner?

CNSS

Whose approval is needed?

A seventeen-step process is used for unanimous approval of each change.

How often is it updated?

They are scheduled for update every three years.

Does it conform to the ISO 17024:2003 Personnel Certification Accreditation standard?

Conforming to 17024 is not in the mission of the organization and is not the intent of the document.

What is the current reach or impact? In other words, how many agencies are using it? How many people/practitioners are certified?

- CNSS community
- Center of Academic Excellence (CAE/IAE) program
- 106 CAE schools

What is the value of the standard as it relates to the IA Educational effort/initiative?

These standards have played a leading role in establishing the new academic growth in the US.

3.2.4 DoD Directive 8570

Executive Summary

The goal of DoD Directive 8570.1, IA Training, Certification and Workforce Management, and its implementing manual, 8570.01-M, *IA Workforce Improvement Program (IA WIP)* is to establish an IA professional workforce with the knowledge, skills and abilities to effectively prevent, deter and respond to threats against DoD information, information systems and information infrastructures. The program leverages the commercial certification industry to provide a baseline of knowledge and skills, and encourages commercial certification providers to meet ISO standards. Primary objectives of the IA WIP are:

- Certify the Workforce: Establish baseline certifications across the enterprise and certify the workforce according to those baselines
- Manage the Workforce: Provide the tools to facilitate both Component management of its IA workforce and the insight of the Office of the Secretary of Defense (OSD) into DoD's overall workforce status and certification posture
- Sustain the Workforce: Enable the DoD workforce to receive continuous learning opportunities to keep their skills current to combat new network threats
- Extend the Discipline: Infuse IA into professional education programs to expand operational leadership's attention to the domain
- Evaluate the Workforce: Establish means of assessing compliance and measuring program effectiveness

What is it? (standard/recommendation/guideline/other) And is it mandatory or optional?

DoD 8570.1 and DoD 8570.01-M comprise DoD policy. As of December 2004, it is mandatory for all DoD personnel performing IA functions, who have privileged access to DoD systems, to meet baseline personnel certification and training requirements outlined in policy.

Who is the target audience? Who are the stakeholders?

Currently, the program impacts over 86,000 military, civilian and contractor staff regardless of whether they perform the IA function full-time, part-time or as an embedded duty. The IA workforce structure is defined in three managerial and three technical categories. Stakeholders include the DoD CISO, Service/Agency CIOs, operational leadership, IA Managers, all personnel performing IA functions as well as end users who require IA literacy/awareness.

Mechanisms/provisions for its update: Who is the owner?

The Policy owner is the Office of the Secretary of Defense, Chief Information Officer, Defense-wide Information Assurance Program (OSD CIO DIAP).

Whose approval is needed?

Approval is required by every Service and Agency in the Department of Defense. The policy staffed and must be approved by all components.

How often is it updated?

The policy is reviewed on an annual basis. Change 1 to the manual has been published, while Change 2 is under development. Advisory Council members comprised of Service and Agencies representatives at a minimum meet on a quarterly basis to policy implementation, including potential modifications to commercial certifications included in the Manual.

Does it conform to the ISO 17024:2003 Personnel Certification Accreditation standard?

In order for commercial certifications to be considered for inclusion in the DoD 8570.01-M they must meet the ISO 17024 standard for certifying bodies. Implementation of this DoD policy has encouraged commercial certification providers to "raise the bar" on meeting ISO standards.

What is the current reach or impact? In other words, how many agencies are using it? How many people/practitioners are certified?

The entire DoD has adopted this program. Currently, the program impacts over 86,000 military, civilian and contractor staff across the enterprise. The program serves as a model for other Federal Agencies. To date nearly 20,000 personnel are certified across the enterprise. The goal is to reach 100% certified by 2011.

What is the value of the standard as it relates to the IA Educational effort/initiative?

The DoD 8570 has aligned functional requirements with baseline certifications, training, operating system certifications, and on the job check rides to produce a verified, competent and professional workforce for DoD by 2011. Through an annual job task analysis/IA skill standard assessment, the Department has identified and verified the functions required to be performed by the core IA workforce. These were verified in 4 separate studies and have stood the test of time for five years. The program serves as a model for establishing baseline skill standards for IA professionals.

3.2.5 DHS Information Technology Security Essential Body of Knowledge (EBK)

Executive Summary

The goal of Information Technology (IT) Security Essential Body of Knowledge (EBK) is to establish a national baseline representing the essential knowledge and skills IT security practitioner should possess to perform. The emerging threat of sophisticated adversaries and criminals seeking to compromise Internet systems underscores the need for well-trained, well-equipped IT security specialists. The EBK effort was launched to advance the IT security training and certification landscape and to help ensure the most qualified and appropriately trained IT security workforce possible. Primary objectives of the IT EBK are:

- Articulates functions that professionals within the IT security workforce perform in a common format and language that conveys the work, rather than the context in which work is performed (i.e., private sector, government, higher education)
- Provides a reference for comparing the content of IT security certifications, which have been developed independently according to varying criteria
- Promotes uniform competencies to increase the overall efficiency of IT security education, training, and professional development
- Offers a way to further substantiate the wide acceptance of existing certifications so that they can be leveraged appropriately as credentials
- Provides content that can be used to facilitate cost-effective professional development of the IT security workforce, including skills training, academic curricula, and other affiliated human resource activities.

What is it? (standard/recommendation/guideline/other) And is it mandatory or optional?

The EBK is a conceptual framework that was shared with focus groups comprised of both IT security generalists and SMEs who represent specific roles reviewed the functional perspectives for each competency and role mapping. As the result, the first draft of the EBK conceptual framework was created and compiled in December 2006. DHS-NCSD introduced this first draft to a broader audience of SMEs in January 2007. It will be re-evaluated approximately every two years to ensure that content and overall structure remains relevant and useful. The EBK is used to further clarify key IT security terms and concepts for well-defined competencies; identifies generic security roles; defines four primary function perspectives; and establishes an IT Security Role, Competency, and Functional Matrix. The EBK is not an additional set of guidelines, and it is not intended to represent a standard, directive, or policy by DHS.

Who is the target audience? Who are the stakeholders?

The IT Security EBK is for use across the public and private sectors. Stakeholders include DHS-NCSD, DoD, academia, and private sector leaders in the IT and information security fields as well as end users who require Information Technology Security literacy/awareness.

Mechanisms/provisions for its update: Who is the owner?

The EBK owner is the Department of Homeland Security, National CyberSecurity Division (DHS, NCSD)

Whose approval is needed?

Modifications to the EBK need to be approved by DHS-NCSD.

How often is it updated?

The EBK is to be re-evaluated approximately every two years.

Does it conform to the ISO 17024:2003 Personnel Certification Accreditation standard?

EBK does not conform to the ISO 17024:2003 Personnel Certification Accreditation standard.

What is the current reach or impact? In other words, how many agencies are using it? How many people/practitioners are certified?

Currently, the EBK has been widely used by the Department of Energy, starting January 2009. The EBK model is also used as a basis of a current initiative to develop an IT Security Skills Qualifications Matrix by the Chief Information Office (CIO) Council IT Workforce Committee. Based on the DHS IT Security Essential Body of Knowledge (EBK), this model will provide a common framework to enable and foster state government IT security workforce development, education/training, and certification requirements.

3.3 Industry Based Education and Training

Over the years, a variety of industry based and vendor specific IA training and certification programs have been developed to provide the necessary training for personnel in the workforce. This type of training began in the 1960s to address training requirements on specific products and systems, usually with the goal of providing some customer support function. As technology evolved and as computers have become ubiquitous, the number of vendors and training institutions has increased to meet the demands of government and industry. In addition, industrial and governmental customers now have their own personnel whose job is to support various information technology and computer systems and equipment and who frequently need vendor specific training and some knowledge of IA.

There are two categories of vendor training and certifications, those that are vendor specific and those that are vendor neutral. Vendor specific IA training addresses specific products and services, whereas vendor neutral IA training addresses the general IA knowledge areas necessary for a given occupation, e.g. system administrator or systems security certified practitioner. The vendor neutral training was developed after, and now frequently follows, vendor specific training. Current practitioners need the knowledge of specific systems, as well as general knowledge of IA. Just as there are educational institutions that offer vendor specific product training, there are also vendors that offer general educational programs and degrees with significant IA components. These educational programs are generally offered by for-profit entities and are not subject to any accreditation process or body.

Vendor specific training typically provides some of certification that is desired, and increasingly required, by industrial and governmental employers, and also by professional associations. There are several standards bodies, e.g., ISO/IEC, the American National Standards Institute, and the International Accreditation Forum, that establish whether or not vendor training is compliant with various standards in the field. Those organizations that offer the training gain financially by meeting these standards.

The target audience for vendor based training and education in the IA areas is made up of the workforce from industry, government and academia. Because the training is concentrated and often of relatively short duration, it is compatible with those in the work force who are in need of targeted training in an area or a specific vendor product. It also enables current work force members to be retrained or made current in a short period of time. This format also reduces the cost of the training with respect to lost work time.

The primary stakeholders in industry based training are the leads/heads of companies and organizations as they are responsible for the success of their organizations. They must seek a balance between the training and education needed for their employees to be successful and must also manage the costs of the training and education. To date, the stakeholders have primarily been interested in training.

The vendors are the owners of these standards and materials and they are responsible for the update process. As this is pay for service training, it is in their best interest to keep pace with the marketplace and technology. Most have advisory boards with representation from government, industry, and academia.

The numbers of people trained by vendors vary based on the specific subject matter and country. In all cases, however, the role of certifications in the IA workforce is increasingly important. Certifications are being viewed as a validation of an individual's knowledge, skills and abilities in the information security profession. Due the rapid pace of change in IA, maintaining currency is critical and certifications frequently need periodic renewal. Industry training increasingly includes a requirement of annual continuing education.

Another distinguishing feature can be related to the target audience. As mentioned, the leads/heads of organizations are ultimately responsible for the success and well-being of their organizations and, hence, need to acquire a fair understanding of IA in a short timeframe. In contrast, the personnel need to acquire in-depth, tailor-made knowledge with regard to some subordinate goal. Consequently, alongside the mentioned in-depth and/or vendor-specific courses, there exist a number of short courses that target superior decision-makers in order to satisfy their managing needs.

4. ASSESSMENT OF IA EDUCATION

4.1 Assessment Relevance

One of the greatest challenges associated with education and training is to determine what quantifies a measure of success as it relates to the learning that has taken place. Numerous measures exist from standardized testing at the primary school level to oral examinations at the doctoral level. While these methods of examination focus on the individual, they reflect on the quality of instruction of the institution providing the training and education. Assessment of an institution's ability to provide quality education and/or training is increasingly more complex as "quality" is a highly subjective term.

The focus here is more on assessment as it relates to an education or training institution than on the individual. Attention is focused on education and training assessment at levels of higher education and professional training. Institutional assessment is relevant and critically important to stakeholders (students, employers, institutions - education, funding, and professional bodies) in the following three areas: individual satisfaction; employer satisfaction; and institutional satisfaction.

Individual satisfaction deals with the candidate's (student's) satisfaction that he/she is receiving quality education and/or training. Besides the individual learning objectives and how satisfaction is derived, one of the primary individual end-goals is to be marketable and employable. Additionally, licensing as a professional at the local, regional, national, or international level

may be another individual goal. While the individual seeks a level of competency for employment, the employer of the graduate needs to understand and know what the new employee brings to the company in terms of preparatory competency. Additionally, an employer must understand the value of a given body of professional continuing education and training. This is critically important given constrained fiscal and personnel resources. Finally, institutional satisfaction results from its graduates being highly-sought for employment, programs being recognized by peers for exceptional quality, and by receiving accreditation and designation from professional, national and international bodies.

4.2 Processes

The assessment of IA programs is usually conducted through a combination of processes. Some of these take place before the start of the program such as *validation* and some after the program becomes operational such as *accreditation*. In addition, some of these processes are internal such as *periodic program review* and some are external such the US accreditation of academic programs containing IA content. Furthermore, some of these processes can be further categorized as "generic" such as program validation and institutional accreditation and as "subject specific" such as program accreditation. Although the similarity of some evaluation processes, such as validation and professional accreditation, are apparent across the US, UK, Sweden and Australia, it is important to recognize substantial differences in country specific processes. For instance, in the UK there is a "generic" system of external examination in which the operational implementation of each program is reviewed by academic peers from other UK universities. This provides mechanisms to assist in maintaining consistency in the quality of degrees level across the country.

4.2.1 Internal Subject Review (validation)

This is a generic process adopted by universities around the globe to assess new programs and to periodically review an existing program or a cluster of related programs. Elements of the validation include student feedback, potential employer input, as well as input from internal and external subject matter experts and university quality assurance officials. There are guidelines of good practices, such as the recent report [30], outlined by the UK Quality Assurance Agency (QAA) for Higher Education [31].

The IA subject specific component of this process may involve evidence that show the program offered conforms to guidelines set by formal bodies (e.g., ACM, ABET, the British Computer Society, etc.), meets recent recommendations set by international IA educational task forces and covers issues and concepts identified by IA professional bodies (e.g., SANS [27] and $(ISC)^2$ [28]).

For instance, in order to substantiate a claim that a student who successfully finishes the program is likely to pass $(ISC)^2$, a piece of evidence may involve defining a mapping that shows how key concepts outlined in $(ISC)^2$ are covered in the program.

4.2.2 Accreditation

Universally, institutions of higher learning seek and gain accreditation of degree programs, as well as institutional operations. This is obviously a wide-accepted practice given the need for stakeholder buy-in for the reasons provided above. In the US, institutional accreditation is generally granted by regional accreditation authorities (e.g., the North Central Association of Colleges and Schools, The Higher Learning Commission--for numerous states in the middle (geographically) of the US). While the US Department of Education [32] does not accredit postsecondary educational institutions, it does, by law, recognize those bodies tasked with conducting the accreditation process. Similarly, in Australia, the Australian Universities Quality Agency [33] is charged with conducting periodic reviews of the thirty-seven state and government supported institutions. In Sweden, the Swedish National Agency for Higher Education [38] is responsible for granting the right to award degrees, and for evaluating main fields of study and study programs every sixth year. In the UK, the Quality Assurance Agency (QAA) for Higher Education [31] is responsible for institution accreditation. The UK Department for Education and Skills maintains a list of all bodies that have their own degree awarding powers and all bodies that currently teach a course which leads to the award of a degree from a recognized body. QAA is a member of the European Association for Quality Assurance in Higher Education (ENQA). Schools, such as those related to business, can be accredited by the Association to Advance Collegiate Schools of Business [34].

While the regional and institutional level accrediting bodies examine individual degree programs for content and consistency with institutional practices, in-depth subject area analysis is not normally associated with these bodies. The detailed area analysis is generally associated with bodies such as Computing Sciences Accreditation Board (CSAB) [35] and the Accreditation Board for Engineering and Technology (ABET) [29]. These bodies accredit degree programs (Computer Science, Computer Engineering, Electrical Engineering, other engineering discipline as well as electronic and engineering technology programs) for periods of time between three to six years. Periodic reviews and self-assessments (internal and external) are associated with these evaluations.

While the above referenced accreditation bodies have mature evaluation and accreditation processes for well-established disciplines, the relative newest of IA does not allow for independent assessment. IA is by nature multidisciplinary. It spans technologies, people, practices, and processes which translate into crossing established disciplines of engineering, science, business, and social sciences.

4.3 Information Assurance Education and Training Assessments

As aforementioned, educational program assessment as it relates to IA is very loosely tied to accreditation of Computer Science, Computer Engineering, Electrical Engineering, and engineering technology programs. Due to the relative newness of the field of study, to date, no accrediting body specifically considers or examines IA as an independent program of study.

While there does not exist formal accreditation for IA programs, extensive efforts have taken place to mature the field of study and to assess the quality of the programs offering the education. In the late 1990s, the United States government realized the need for IA professionals and the lack of available educational programs to meet those needs. Motivated by the Presidential Decision Directive 63 [24], National Policy on Critical Infrastructure Protection dated May 1998, a national program was established focusing on reducing vulnerability in U.S. national information infrastructure by promoting higher education in IA, and producing

a growing number of professionals with IA expertise in various educational disciplines.

The National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) Program [13] is jointly sponsored by the National Security Agency and the Department of Homeland Security and is open to nationally or regionally accredited 4-year colleges and graduate-level universities. To become a CAE/IAE, an institution must go through a rigorous two phase evaluation process. First, an applicant institution must map its IA curricula to at least two of the national training standards: the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4011 National Training Standard for Information Security (INFOSEC) Professionals and at least one of the Committee on National Security Systems standards (CNSS 4012-4016) [25]. This courseware mapping ensures curricula content designed to meet the needs of the U.S. Federal Government. Courseware assessment is examined and mapped at the awareness, knowledge, and comprehension levels. The second phase of the CAE/IAE designation process is for the institution to show a comprehensive capability and competency in IA education, practice, and outreach. The following evaluation criteria for CAE/IAE designation have been established:

- *Outreach/Collaboration:* To ensure the national awareness and growth of IA education and practice, an applicant institution must show that its programs extend beyond the normal boundaries of the University and bring current IA practitioners into the IA Center. Applicant institutions must provide evidence of partnerships in IA education with minority colleges and universities, or K-12 schools, or 2-year community colleges, or technical schools.
- *IA as a multidisciplinary science:* An applicant institution must show that IA is not treated as a separate discipline, but as a multidisciplinary science with the body of IA knowledge incorporated into various disciplines.
- *Practice of IA encouraged throughout the University:* An applicant institution must show evidence that it encourages the practice of IA, not merely that IA is taught.
- *Student-based IA research:* An applicant institution must demonstrate student-based IA research is being conducted as it fuels the relevancy and currency of IA curricula.
- *Faculty active in current IA practice and research:* An applicant institution must demonstrate that its faculty practices IA, performs IA research, and contributes to IA literature.
- *IA Resources:* An applicant institution must demonstrate that the faculty and students have access IA resources and reference materials.
- *IA academic program exists:* An applicant institution, which is a nationally or regionally accredited 4-year college or graduate-level university, must demonstrate that it possesses an academic program with an area of study or focus area in IA.
- *Center for IA Education:* An applicant institution must have a declared center for IA education or a center for IA research from which IA curriculum is emerging. The center may be school or university-based.
- *Number of IA faculty and course load:* An applicant institution must demonstrate the active involvement of faculty in the IA curricula.

Once meeting the assessment criteria outlined above, an institution is designated as a CAE/IAE for a period of five years. Reapplication for subsequent designation is required and should occur midway through the fourth year of the current designation period. In 2008, the CAE/IAE program was expanded to include research-centric institutions (CAE-R). Presently, there are 106 institutions across the United States designated as a CAE/IAE, CAE-R, or both.

4.3.1 Commercial IA Training Assessment

The market initially drives the number of commercial IA training venues. By this, if there is a determined demand for a given product, commercial entities will be formed to meet this demand. Most of these commercial venues either provide some type of certification or courseware/instruction that leads to the ability to obtain a certification. These certifications can be vendor specific such as a Cisco router certification to vendor neutral certifications such as the Certified Information Systems Security Professional (CISSP). The certification by security professional bodies continues to grow and currently enjoys wide recognition by employers in specific domains. The main target audience is those professionals who have had several years in employment in IT security domains and would like to have formal recognition of their knowledge and skills in specific IA subjects. Currently, there are several certification programs offered by professional bodies. The most prominent certification in information security is provided by the International Information Systems Security Certification Consortium ($(ICS)^2$). In addition, there are several certifications offered by the BCS (information security, and information risk management) and ISACA (information security, auditing). More specialized qualifications are offered by Cisco in security of network communications and configurations, and by the Systems and Network Security (SANS), in secure programming, network security, vulnerability discovery and identification and treatments in specific programming frameworks such as Java, C#, .Net and C++.

As with the educational assessment of "quality" IA programs, there does not exist a universally accepted and standardized assessment process/standard for commercial IA training. Lacking this universal assessment process, criteria to consider in assessing the quality of a commercial training program can include [26]:

- How long has the certification been in existence?
- Does the certification organization's process conform to established standards?
- How many people hold the certification?
- How widely respected is the certification?
- Does the certificate span industry boundaries?
- What is the probability that 5 or 10 years from now, the certificate will still be useful?
- Does the certification span geographic boundaries?

4.4 Success Metrics

As previously discussed, assessment of "quality" in education and training is a difficult task. Similarly, defining success metrics in education and training can also be highly subjective. From a U.S. perspective, given the PDD 63 guidance from 1998 to increase the number of IA professionals employed within the Federal government, an obvious educational success metric is the number of IA graduates who have entered Federal government service. On the broader scale, IA graduates will be or are needed and are being employed within industry, academia, and government around the globe. This primary metric (number of graduates) leads to secondary metrics such as the number of academic institutions that have emerging or established academic programs in IA, producing new educators via doctoral programs and increased collaborative efforts (curricula development and research partnerships) to advance the field of study. From an industry training perspective, the success metric lies in the number of individuals enrolled in specific courses and certification programs.

The number of IA professionals being produced for US government employment is predominantly being accomplished via the NSF SFS program and the DoD IASP. Beginning in 2001 and through 2008, 1001 (852 in SFS, 149 IASP) students have received IA scholarships and have graduated via sponsorship from the aforementioned programs. Of these graduates, 93% have gone on to receive jobs and work for the Federal government. While successfully increasing the number of IA professionals employed by the Federal government, these numbers reflect only a small percentage of the approximately 8,000 projected new IA/cyber hires needed by the Federal government over the next four years. It is unknown what the global demand for IA professional in industry and academia will be over the same period of time, but these sectors will compete to employ a relatively scarce resource. The scarcity of quality IA professionals continues to drive the need for expansion of IA academic across the globe. The US government emphasis on IA has been a prime motivator in this expansion as the number of academic institutions with IA programs or emphasis that have been designated as a CAE/IAE and/or CAE-R has grown from 7 in 1999 to 106 at the present time.

Rapid growth in the number of individuals certified by vendor neutral training may be the most prominent assessment measure with other aspects of the above criteria inherently embedded. For example, the Systems and Network Security (SANS) Global Information Assurance Certification (GIAC) has been awarded to over 26,000 individuals since its founding in 1999 [27]. The fastest growing and broadest certification is the CISSP designation. It has been granted to 61,000 individuals since its inception in 1988 [28]. In its latest version of its *Information Assurance Workforce Improvement Program*, U.S. DoD 8570 recognizes the need for professional certification for its workforce and calls for increasing percentages of its workforce to obtain these certifications in the upcoming years.

5. CHALLENGES AND FUTURE DIRECTIONS

It is clear from the previous sections that IA has matured considerably over the past three decades and is now on the verge of being recognized as its own discipline. The number of faculty and programs that identify themselves as participating in IA continues to grow, there is an increasing body of scholarly work in IA, and a common set of student learning outcomes and courses topics is beginning to precipitate out from the many existing IA curricula and standards. As IA begins the last steps towards formal definition and recognition as a discipline, it faces many challenges.

First and foremost, there is the need for some governing body, such as the ACM or IEEE, to work with IA educators and practitioners to develop education models for 2-year, 4-year and graduate level degree programs. The governing bodies also need to work with the IA community to develop formal mechanisms for the continual improvement of these programs and possibly for some form of accreditation. In doing so, the governing body must respect the diversity and interdisciplinary nature of extant IA educational programs and be cognizant of the important role that government and industry standards have played in shaping the content of the field. This working groups calls for the creation of an IA Educators body to study these issues.

As the demand for IA professionals at all educational levels continues to rapidly grow, it is clear that academia will soon face a dramatic shortfall of faculty with the proper qualifications to educate students to meet this demand. This is particularly true in the US where the government is likely to make large investments in programs to foster student education and training in IA. Government, industry and academia must come together immediately to explore creative mechanisms for increasing the IA faculty pipeline.

Another challenge (likely only a challenge in the US) not unique only to IA education is academic credit articulation from the lower academic division (typically completed as part of a community college program) into the upper division (typically completed as part of a baccalaureate program). Transfer-oriented associate-degree programs rely on formal inter-institutional articulation agreements to ensure that students experience a seamless transition between lower division associate degree coursework and upper division baccalaureate degree coursework. Articulation of courses and programs between two academic institutions facilitates the transfer of students from one institution to the other. Effective articulation requires a close evaluation of well-defined course and program outcomes as well as meaningful communication and cooperation. Many associate degree courses in IA, often taken towards accomplishing industry-based certifications do not easily transfer into baccalaureate programs. Guidelines and standards for IA education will likely facilitate this much needed articulation.

Even more seriously, it is likely too late to wait until college before introducing students to IA. It is clearly the case that aspects of IA can be introduced into the K-12 (or secondary school) classroom. Much more educational work is needed in this area.

Finally, the IA community must consider the role that licensure and certification will play in the IA profession vis-à-vis IA educational programs. Historically, IA education programs have been strongly influenced by industry and government training standards, many of which lead to some form of certification, and this is likely to continue for the foreseeable future. It is not clear, however, that all or any IA degree programs need to have some form of certification or licensure as a specific intended outcome of the program. As the academic community moves towards formalizing IA educational models and industry and government continue to promulgate IA training standards, the tension between

these two is likely to increase unless the entire community engages in a dialogue that clearly articulates the role that certification and licensure will have in the broader IA endeavor.

6. CONCLUSION

Information Assurance is a serious worldwide concern of governments, industry, and academia. The purpose of this working group, and the document produced has been to explore existing academic guidelines and industry and government standards and guidelines for Information Assurance education, and how they may serve as a basis for solidifying the burgeoning discipline of Information Assurance. This document provided an historical context for Information Assurance, describing its origin and highlighting its important milestones along the way. Education guidance from existing academic bodies of knowledge, government standards, and industry certifications across the globe demonstrated the growing demand for information assurance professionals and technicians. The discussion of the assessment and accreditation of current education and training programs established the relevance and currency of information assurance to interested stakeholders. In conclusion, this paper has laid the groundwork in support of Information Assurance as a discipline in its own right. However, the authors of this working group recognize this elucidation as only the first step of many to come and close with future directions and challenges facing the emerging discipline of Information Assurance.

7. REFERENCES

[1] Computing Curricula 2005, The Overview Report (http://www.acm.org/education/education/curric_vols/CC2005-March06Final.pdf)

[2] Information Technology 2008, Curriculum Guidelines for Undergraduate Degree Programs in Information Technology (http://www.acm.org//education/curricula/IT2008%20Curriculum.pdf)

[3] Computer Science 2008, An Interim Revision of CS 2001 (http://www.acm.org//education/curricula/ComputerScience2008.pdf)

[4] Software Engineering 2004, Curriculum Guidelines of Undergraduate Degree Programs in Software Engineering (http://sites.computer.org/ccse)

[5] Computing Curriculum 2001 (http://www.acm.org/education/curric_vols/cc2001.pdf).

[6] Samuel T. Redwine, Jr., Editor. (2006). *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software Version 1.0*. US Department of Homeland Security, May.

[7] http://www.swebok.org

[8] The "CORE Body of Knowledge for Information Technology Professionals" (http://www.acs.org.au/ictcareers/index.cfm?action=show&conID=cbok3)

[9] *Report of the Task Force on the ACS Towards 2000,* Australian Computer Society, November 1992.

[10] Computing Curricula 2009: Guidelines for Associate-Degree Transfer Curriculum in Computer Science. http://www.acmtyc.org/WebReports/CSreport/

[11] ACM Education Curriculum Recommendations. http://www.acm.org/education/curricula-recommendations

[12] ACM TYCEC Curriculum, Assessment, and Pedagogy repository. http://www.capspace.org/

[13] NSA list of CSEs http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

[14] SFS program solicitation http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5228

[15] IASP program description http://www.defenselink.mil/cio-nii/sites/iasp/

[16] NSA IASP program requirements http://www.nsa.gov/ia/academic_outreach/nat_cae/cae_iae_program_criteria.shtml

[17] National Training Standard for Information Systems Security Professionals http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf

[18] NIST 800-16 Standard http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

[19] DoD 8570 Directive http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

[20] DHS EBK http://www.us-cert.gov/ITSecurityEBK/EBK2008.pdf

[21] ISO 17024 Standard http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29346

[22] IFIP WG 11.8 homepage http://www.118.ifip.info/

[23] IFIP TC11 WB 11.8 Information Security Education, Proceedings WISE 2, 2nd World Conference Information Security Education, Edith Cowan University, Perth, Western Australia, July 12-14, 2001.

[24] http://ftp.fas.org/irp/offdocs/pdd/pdd-63.htm

[25] http://www.cnss.gov/

[26] J. Ryan and C Schou (2004) *On Security Education, Training and Certifications.* Information Systems Control Journal. Volume 6.

[27] http://www.sans.org

[28] http://www.isc2.org

[29] http://www.abet.org

[30] http://www.qaa.ac.uk/reviews/ELIR/GoodPractice/InternalSubjectELIR.pdf

[31] http://www.qaa.ac.uk

[32] http://www.ed.gov

[33] http://www/auqa.edu.au/

[34] http://www.aacsb.edu/accreditation/

[35] http://www.csab.org/

[36] C. Schou, W. Maconachy, et al. (1993). *Organizational Information Security: Awareness, Training and Education to Maintain System Integrity*. In Proceedings of the Ninth International Computer Security Symposium. Toronto, Canada.

[37] B. E. Mullins, T. H. Lacey, R. F. Mills, J. M. Trechter, and S. D. Bass. (2007) *How the cyber defense exercise shaped an information-assurance curriculum*. IEEE Security & Privacy, 5(5):40–49, Sept.– Oct.

[38] http://www.hsv.se/

[39] http://csrc.nist.gov/groups/SMA/fisma/index.html

[40] L. Hoffman (1974). *Course outline for computer security and privacy.* SIGCSE Bull. 6, 3 (Sep. 1974), 13-17.