A Critical Analysis of the Centers of Academic Excellence Program

Matt Bishop
University of California at Davis
mabishop@ucdavis.edu

Carol Taylor
Eastern Washington University
ctaylor@mail.ewu.edu

Abstract

The US National Security Agency (NSA) established a program in Information Assurance education in 1999 that established Centers for Academic Excellence in Information Assurance Education (CAEIAE). While designated a success by the government, the program has been criticized over the years by program participants as less than optimal. In this paper, we review the program and identify the most serious problems. We then suggest possible solutions to these problems in order to improve the program so that it represents true excellence in IA education.

Index terms – Security Education, Curriculum Standards, Centers of Academic Excellence in Information Assurance Education

I. Introduction

Times have changed. In 1997, when the first National Colloquium on Information Systems Security Education (NCISSE) was held [4], the threats to the Internet and nation's infrastructure, and personal computer systems, were nowhere near as serious as the current threats. Spam and malware, while common, was not yet the prevalent form of electronic mail. Botnets and zombies were relatively rare. Academics discussed cyberwarfare; if it was practiced, it was practiced in classified arenas. One serious debate concerned whether "red teaming" was a legitimate topic of study in school, with the consensus being split between supporting the need to learn those techniques in order to defend against them, and believing that teaching those techniques was highly unethical. Now, zero-day worms are real, and not just a topic of academic discussion. The threat of spam has diminished; now, phishing and its variants present far more danger to users, particularly naïve ones. Botnets, which consist of networks of thousands of hosts controlled by malicious attackers, are one of the fastest growing menaces on the Internet. These networks are capable of launching DDoS attacks, untraceable spam relays, and widespread malware attacks [6].

Statistics from a 2007 report from McAffee, a leading anti-virus company, indicated well over 100,000 new viruses and Trojans, a 50 percent jump in the total number of threats ever cataloged. Other highlights include the Nuwar virus (a.k.a. Storm Worm) grew into the largest peer-to-peer (P2P) botnet to date, while the data breach at TJ Max which occurred undiscovered over a period of several years compromising thousands of customer credit cards was the largest data breach in history [7]. Spafford, a well-known researcher and educator in computer security, commented that the same problems that existed in 1988, were still very much present in 2003 and have not yet been remedied [13].

In 1997, the academic keynote at the NCISSE [2] called for more and better academic information assurance and computer security programs to educate students in this area. To help fill this need, in 1998 the National Security Agency began a program to recognize those institutions working in this area. The institutions were designated "Centers of Academic Excellence in Information Assurance Education" (CAEIAE) [10]. The original goal of this program was to increase the number of students educated in information assurance, to create centers of computer security knowledge for education, and to provide a resource to which the nation could turn in order to improve the state of computer security and information assurance. Faculty at the centers would then perform outreach to surrounding institutions in an advisory capacity or as visiting faculty. The importance of this program was recognized by the Department of Homeland Security's becoming a co-sponsor of the program when that Department was created. Now, 11 years later, the need for graduates from computer science programs to be educated in information assurance, and the faculty to teach them, is stronger than ever.

If the measure of success of the CAEIAE program is the number of centers and their distribution throughout the United States, the CAEIAE program is successful. Over the 10 years of the program, the number of centers has grown from the original 7, distributed over 5 states, to 93 distributed over 37 states and the District of Columbia [10]. Thus, the number of students graduating from CAEIAEs is increasing, satisfying the goal of producing more computer security professionals who have been exposed to information assurance.

But that metric does not measure the other goals behind the CAEIAE program. Have the Centers of Excellence increased the number of students who are expert practitioners of information assurance, or who have a deep understanding of information assurance? Has the creation of CAEIAEs increased the number of faculty in the field? Are the CAEIAEs centers of computer security information and knowledge, and research? Do they provide a resource to which the nation, and industry, can turn to improve the state of computer security and information assurance?

We contend that the benefits of the CAEIAE program could be greatly enhanced, and the ability of the program to meet these other goals greatly strengthened, with some basic changes to the program. The changes are not extensive, but they do require a change of mindset, in which measuring the goals moves away from simple metrics. The funding commitments would be minimal; the time commitment of the government agencies administering the program would be greater. The results would be well worth the effort.

The purpose of this paper is to review the CAEIAE program with regards to its goal of establishing academic centers of excellence in information assurance, identifying specific areas for improvement, and offering suggestions for improvement. We review both the programs strengths and its weaknesses and propose solutions which we believe will create a stronger, more effective program.

The authors emphasize that the goal of this paper is *improvement*. Both authors strongly support the CAEIAE program and its spin-off, the CAE-R program. Indeed, one of the authors (Bishop) has been a co-director of the UC Davis Computer Security Laboratory, which leads the CAEIAE effort for the University of California at Davis, and has worked with the program since its inception. Our criticisms and suggestions are offered in the spirit of wanting this program to achieve its goals.

The paper begins with a history of the CAEIAE program and computer security education, followed by a brief review of the CAEIAE program and a discussion of the process for becoming a Center of Excellence. We use this review as the basis for presenting the weaknesses of the CAEIAE program. The next section presents suggestions for ameliorating or resolving the problems. The paper concludes with a summary and concrete recommendations for improving the CAEIAE program.

II. History of Information Assurance Education

Before the creation of the CAEIAE program in 1998, IA education was not common within academic programs. Early academic programs were primarily aimed at graduate students. Early courses mirrored US government research interests and included discussions of multi-level security (MLS), information flow models, covert channel analysis and the design of high assurance systems [2]. There was little emphasis on practical topics such as secure system management, network security, and secure coding.

The CAEIAE program was conceived as a way to encourage students to become information security professionals. The program began in 1998 and the first seven Centers of Academic Excellence (see Figure 1) [10] were named in 1999. At that time, the US government felt that there was a shortage of information security professions and the CAEIAE program was proposed as a solution to this problem.

School
James Madison University
George Mason University
Idaho State University
Iowa State University
Purdue University
University of California at Davis
University of Idaho

Figure 1. Original Seven Centers of Excellence

Most of these first seven centers were active in research and have graduate programs capable of producing future IA faculty. Since its inception, each year the CAEIAE program has added schools as centers until at present time there are 93 schools in the CAEIAE program.

The goals of the program are twofold: "to reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA), and producing a growing number of professionals with IA expertise in various disciplines" [10]. In practical terms, this means increasing the number and quality of practitioners of students and faculty in the field of information assurance, encouraging and assisting the growth of research and education in that field, and developing centers that can assist government and industry in their efforts to improve the state of the security of the national information infrastructure.

A. Process of Becoming a Center of Excellence

To become a CAEIAE, an institution maps the content of its courses to the CNSS training standards. The IA Courseware Evaluation Program (IACE) reviews the mappings, and if found satisfactory provides official recognition for those schools [9,11]. The school must cover the material in training standard 4011. The 4011 standard covers a set of knowledge considered basic to knowing information security. The school must also show

its courses map into at least one other standard that requires more specialized knowledge. The CNSS standards 4012-4016 are described in Table 1.

Table 1. CNSS Training Standards

Standard Name	Year	Description
NSTISSI 4011	1994	Information Systems Security Professionals
CNSSI 4012	2004	Senior Systems Managers
CNSSI 4013	2004	System Administrators in Information Systems Security
CNSSI 4014	2004	Information Systems Security Officers (ISSO)
NSTISSI 4015	2000	System Certifiers
CNSSI 4016	2005	Risk Analysis

The stated purpose of the IACE program is "to expand the use of national standards in information assurance education and training throughout the nation. These standards were developed for the government, but have been kept unclassified to share with the greater IA community" [9]. It provides an assessment of the degree to which courseware from commercial, government and academic sources maps to the national standards. Thus, the IACE program's purpose is much broader than academic compliance, also extending to government and commercial training programs.

Once a school has mapped their courses to the CNSS standards, it must meet other requirements to become a CAEIAE. These criteria are intended to measure the depth and maturity of programs of instruction in information assurance at the graduate and undergraduate levels. Figure 2 lists these criteria. The school provides information and references to enable external evaluators to examine the information and determine whether it is sufficient to meet the criteria for a Center of Excellence.

Once a school is designated a CAEIAE, it must recertify every 5 years. The recertification process is essentially a re-application, in that the school must show it continues to satisfy the CNSS requirements as well as the other requirements.

Ten Criteria for Centers of Academic Excellence

1. Partnerships in IA Education
2. IA Treated as a Multidisciplinary Science
3. University Encourages the Practice of IA
4. Academic Program Encourages Research in IA
5. IA Curriculum Reaches Beyond Geographic Borders
6. Faculty Active in IA Practice and Research and Contribute to IA Literature
7. State-of-the-Art IA Resources
8. Focus area or area of study in IA
9. Declared Center for IA Education or Research
10. Full-time IA Faculty

Figure 2. Criteria for CAEIAE designation

III. CAEIAE Program Weaknesses

Assessing the success of the CAEIAE program is difficult. If one believes that the more Centers there are, the more security professionals will be produced, then the increase in the number of Centers would demonstrate that the program is wildly successful. But such reasoning assumes a correlation between the number of Centers and the number, and quality, of graduates of those Centers with expertise in information assurance. So the number of Centers alone provides an inadequate measure of success.

Another goal of the program is to establish centers of expertise that serves as a resource for program development and as centers for IA research. There has been criticism from program participants regarding the criteria used to establish these centers, the recertification process and the level of funding and support after a center is created. Each of these criticisms will be examined in the following sections.

A. CAEIAE Designation and Renewal

One of the most time consuming aspects of the process for a school to become a CAEIAE is in performing the curriculum mapping to the CNSS standards. There are two aspects to this: the mechanical process of providing the information, and—more seriously—the standards against which the information is certified.

The first problem is annoying, but easily remedied. The mapping process itself is extremely time consuming and this entire lengthy process must be repeated when the school needs to recertify. When the standards change, prior information is lost, so for many schools there is no way to update the previous certification. Consequently, recertification is as daunting as the original effort.

Dealing with the second problem, the use of the CNSS

standards, is more difficult. College level undergraduate and graduate courses differ significantly in purpose and content from professional training standards, and the correspondence is often not clear. A survey of CAEIAE participants showed that schools had to use multiple courses to satisfy one CNSS standard [16]. Worse, participants noted that certain components in the standards did not map to any of their existing courses because the material was highly specific to the government work environment [16]. Thus, a great deal of time is spent trying to show correspondence between specific skills-oriented training standards and the more generalized content of undergraduate college level courses.

Previous studies documented problems with the CNSS standards [15,16]. One paper detailed how the one required standard, NSTISSI 4011 was deficient as a model curriculum for college courses because of its lack of generality, dated material and incomplete content [16].

A follow-up study presented results from a survey of schools that had completed the IACE courseware mapping in which schools were asked to evaluate the mapping process and the CNSS standards. Results from the survey indicated that a majority of respondents felt that the CNSS standards did not provide good guidance for either undergrad or graduate education. Survey responses indicated that the standards are out of date and fail to address many important areas of information assurance [16].

The main problem with using NSTISSI 4011 as a guide to college level curriculum development is that the goals of NSTISSI 4011 are fundamentally different than those of academic education. Briefly, the goal of NSTISSI 4011 is to ensure students are trained in specific topic areas related to the job they will perform should they be hired by a government agency. This type of knowledge may be inapplicable in other areas (including many security jobs in industry). Academic education emphasizes fundamental understanding of principles and concepts, and how to apply those principles and concepts to specific situations. For example, a security professional trained in managing infrastructure can deploy and configure routers and DNS servers to secure a network. But when asked to secure a Linux system, that professional may not understand how to do it without substantial retraining on both Linux systems and the difference between network-centric defense and host-based defense. By way of contrast, a security professional with a strong academic education in information assurance will need some training in both situations, but considerably less than the trained security professional, because her understanding of principles and concepts will enable her to take much of the information from the network-oriented situation and apply it to the host-oriented situation. The cost of academically educated people is some initial training (although there are various ways to minimize this); the benefit is an employee who is flexible and able to apply her learning to new situations [18].

To sum up, there are educational objectives and outcomes that go beyond specific information assurance training goals that should be incorporated in a college level curriculum standard. General outcomes desirable from a college educational program of study include communication skills both written and oral, problem solving, critical thinking, and interpersonal skills [17]. Ideally, recommendations on course sequencing or integration with existing programs would be included in a recommended IA course of study.

B. Lack of Resources for the Centers

Funding for the centers has been a concern from the program's inception. Currently, the being designated a "Center" brings with it no government support for administrative overhead, security research or faculty development. The lack of funding creates a hardship for Centers that typically have one or two faculty who must then administer the program in addition to other duties such as course development, graduate student mentoring and research.

The lack of funding for centers and information assurance education in general has been called a major barrier to the development of academic information assurance programs. In 1997 and in 2000, Bishop discussed how the lack of a stable funding base adversely affects computer security programs [2,3]. While funding for cyber security research has improved slightly in the past 10 years, it is nowhere near the level needed to sustain the Centers. NSF offers grants for information assurance but they are highly competitive with an acceptance rate of between 10 – 12%. Consequently, new professors are discouraged from entering an area of research with little opportunity and established faculty must constantly search for funding as opposed to devoting their time to research projects. The security industry has also commented on this lack of support for information assurance research. An editor of InfoSecurity magazine commented that the lack of government investment in security research hurts academic programs by discouraging Ph.D.'s from entering the field, which in turn creates shortages of faculty trained in security [1]. The Cyber Security Industry Alliance (CSIA), a group of security vendors, also noted a lack of long-term research funding in a 2005 report [5].

The Information Assurance Scholarship Program (IASP) [8] is a program for supporting students in the area of information assurance. It is funded by the Department of Defense, and students awarded the scholarship go to a

CAEIAE to study. After they graduate, they must work in government service for the same number of years that the scholarship funded them. The NSF's Scholarships for Service program [12] is similar, except that it is not restricted to Centers, and allows only 2 years of support. Thus, these programs are really programs for meeting federal agency needs for security professionals.

Associated with both scholarship programs are capacity-building programs. These provide some additional money for building infrastructure, such as building lab facilities or creation of new courses. The funding levels are low and not intended (and insufficient) for long-term support.

IV. CAEIAE Program Improvement

The previous section described two weaknesses of the CAEIAE program. We emphasize that these weaknesses reduce the effectiveness of the CAEIAE program; they do not render it worthless. Promoting security education and a greater awareness of the importance of information assurance within academia is clearly critical. In that spirit, we offer several suggestions for overcoming the above weaknesses.

A. Use Academic Standards, Not Training Standards

Currently, the Centers are certified against training standards which is not appropriate for academic institutions. If the goal of the CAEIAE program is to build a solid infrastructure of professionals who understand and can teach information assurance, and practice it in a wide variety of jobs, the Centers should be certified against academic, not training, criteria. In particular, the standards should be patterned after something like the ACM/IEEE curriculum [14], and certification should involve an analysis of the courses and material being taught, similar to the curriculum reviews done by accrediting bodies in the academic world (such as ABET).

The actual problem here is that the Centers seem to be serving two purposes. The first is to provide trained professionals that the government can employ with minimum training. The second is to build up the educational and research infrastructure of the nation. The current CAEIAE educational criteria are heavily weighted towards the former. The use of the term "academic" in the title of the program indicates that the designers of the program understood that the latter is crucial to the success of the program.

This suggests two approaches. The first is simply to replace the training standards with academic standards. This would require the development of such standards, and their general acceptance. This should be done in concert with both a recognized non-commercial, non-profit organization such as the ACM or IEEE. Then an accrediting group working in conjunction with the CAEIAE program should perform the analysis of information assurance programs to determine whether the school should be designated a CAEIAE.[1] This type of review will have two immediate benefits. The first is a convergence on the ideas underlying a basic computer security curriculum. There will be great variations in what graduates will know; this will ensure a breadth of knowledge and skills, and a diversity of viewpoints, that will provide the impetus for growth in the field. The second is that the accrediting group members, who work for the CAEIAE program and its sponsors, can give the school extensive feedback on deficiencies that need to be remedied, weaknesses that need to be addressed, and strengths that should be nurtured. This will strengthen arguments that the program will make to the university administration for more resources to address these concerns, and to grow. Also, the sponsors will get direct input from the accrediting group members, rather than the self-reported analyses of courses and research that are currently used.

Another solution to improving the CAEIAE program would be to split the schools into two groups based on their purpose. One designation, the "Center of Academic Excellence in Academia" (CAE-A), would designate schools that provide an excellent education in the academic sense. These would be designated after a review as described in the previous paragraph. A second designation, the "Center of Academic Excellence in Training" (CAE-T) would designate those institutions that meet the existing standards. There is precedent for this type of augmentation. In 2008, 23 universities were designated as "Centers of Academic Excellence in Research" (CAE-R). The above proposal applies a similar division to the types of education.

These designations are not hierarchical; rather, they recognize the two different kinds of education that the CAEIAE program is intended to support. It would also eliminate much of the concern about schools being designated CAEIAEs that are inadequate academically. The problem is that these schools offer fine training programs, but are not "universities" in the academic sense of the word. Designating these CAE-Ts would emphasize their strengths in training, just as designating universities as CAE-As would emphasize the academic education that these institutions offer.

This speaks to a common criticism of the CAEIAE designation: that the institutions designated as CAEIAEs vary wildly in strength. For example, the difference in

[1] The members of the accrediting group evaluating a CAEIAE, or a potential CAEIAE, must be selected to minimize any conflicts of interests. How to do this is not clear; one approach might be to select them from non-CAEIAE institutions.

knowledge and expertise of graduates from institutions with active research programs and doctoral programs in information assurance, and smaller colleges offering a Masters' degree in information assurance, is extreme. Currently, the program treats all schools as equal. Perhaps differing designations, based on the goals and programs, would ameliorate this criticism.

Ideally, the institutions would work together. For example, if a student were to enter government service after graduating from a CAE-A, the student may need some exposure to a particular set of laws or to the application of particular concepts. Then the student could spend a semester at a CAE-T, taking the courses that would give her the training needed. Further, the CAEIAE program could focus on providing appropriate resources for each type of institution. This brings us to our next point.

B. Provide Resources for CAEIAE Institutions

People respond well to incentives. So, in order to advance the agenda of the CAEIAE program, the existing CAEIAEs should be given incentives to grow, and new schools should have incentives to join the CAEIAE program.

Alas, currently the only incentive is the designation, and the ability to host IASP students. This is not sufficient for many schools, especially given the effort to be certified and maintain that certification (see the next section). Compounding the problem is the lack of support for educational programs in general. This means that university programs such as those supporting the CAEIAE goals have insufficient funds to grow, or in some cases even maintain their status.

Several incentives will encourage CAEIAEs to grow and new schools to become CAEIAEs We suggest additional (minimal) funding; access to research projects; a tighter collaboration between government personnel and academic institutions; and incentives for students to enter the ranks of tenure-track faculty. We discuss each in the next paragraphs.

First, academic programs that would get the CAEIAE designation typically have lots of paperwork and administrative work to deal with. This is especially true if the programs are to grow and to be cross-disciplinary. Universities and academic institutions in general are bureaucracies, and like government require some time, skill, and knowledge to work with. An administrative assistant, who would act as a first point of contact for the Center, help administer it, and provide support for the academic and research programs of the Center, would be an invaluable assistant to the Center's growth. It would also release the faculty from many mundane tasks, allowing them to spend more time on teaching, curriculum development, and research. Further, most administrative assistants cost less than a faculty member or a research program, so funding such a person would be relatively inexpensive. And it would make Centers more responsive to requests, because there would be a designated person whose primary responsibility is to keep information flowing between the CAEIAE program and the Centers.

A second alternative, one more appealing to CAE-Rs but possibly of interest to CAEIAEs in general, is to have targeted research programs that only CAEIAEs could apply for. These programs would deal with specific problems in information assurance, and their goal would be not merely to solve immediate problems but also to focus on the long-term problems that will require basic, foundational research to solve. Currently, our research is focused on short-term solutions—which is like using wood to shore up a collapsing bridge. The shoring works for a while, but after time the bridge will collapse regardless of how much support it has. Far better is shoring up the bridge only long enough to build a new bridge that does not suffer from the same structural defects that caused the bridge to collapse in the first place! So, the research programs should have long-term (5 to 10 years, at least) funding for Centers that will give researchers the time to develop and test new approaches to solutions or new paradigms for security, rather than trying to solve "the problem of the day" in a way that cannot solve related problems. This will also address a second, more pervasive problem in research. Short-term research funding expires before students graduate, so its ability to support graduate students is limited. It forces faculty members to focus as much on fund raising, to support their graduate students, as it does on research, to the detriment of the research and the graduate students. This also supports the need for long-term funding.

One aspect of the CAEIAE institutions that has received little notice is the gulf separating many from the government agencies sponsoring, or benefiting from, the CAEIAE program. This is detrimental for two reasons. First, academics frequently do not understand the problems of government agencies, and the constraints under which they function. Second, government employees frequently do not understand how different academic governance and academic institutions are when compared with government. The best way to bridge this gap is to begin a program where government employees can spend a quarter, semester, or year (or longer) at a university, working with the graduate students and researchers, giving guest lectures in computer security classes (or possibly even teaching one). Their specific task would be to build connections, teach, and work with research already under way. This will benefit the students immeasurably, because they will be working with

someone who can show them the immediate application of their research, and who can bring real-world examples into the classroom. It would increase the visibility of the Center within its own academic institution, to the Center's benefit. It would also benefit the government, because it would give them the ability to see what others consider important problems, and how academics approach problems and do research. Similarly, a program that brings academics into government institutions would be salutary, *provided* this could be done in such a way that the academic could bring what she has learned back to the university (in other words, the issue of classified work might pose a problem).

The SEAL program is a good start. That program designated a senior executive to interact with one or more CAEIAE's. Our proposal simply takes this idea farther, and increases the contact between the SEAL and the CAEIAE. In fact, our focus is to increase the contact between the government and the Center.

Finally, consider the problem of encouraging graduate students to become faculty members. Currently, the IASP and SFS programs are obstacles, because once out of graduate school, the student must work for the government for several years—and when they are done with their obligation, their ability to get jobs at research universities is greatly diminished, because they have not been active in research for several years. An alternative is to assert that those who teach the next generation of information assurance professionals are just as valuable to the improvement of the nation's infrastructure as those who work for the government directly. With this point of view, an equally valid goal of both the IASP and SFS programs is to produce teachers as well as government employees. So, the programs could modify the students' obligations to allow them to substitute one year of teaching for one year of government service. This actually fits well with the way the tenure system works at most research institutions. Tenure-track faculty generally go up for tenure after 5 to 7 years as an untenured faculty member. As most Ph.D. programs take 3 to 5 years, by the time the former student goes up for tenure, her obligation would have been paid back.

We emphasize the need here for creativity. Many incentives can be developed; we have suggested some that, based on our experience, we believe would be effective. Critical is that the proposed incentives be evaluated *in light of the academic institution needs and benefits*; these generally differ from what would work in government or industry.

V. Conclusion and Future Steps

The Center of Academic Excellence program, sponsored by the National Security Agency and the Department of Homeland Security, is in crisis. It identifies institutions that have programs considered to be among the best information assurance programs in the nation. But it provides no benefits beyond that designation to the schools. It requires the faculty of the school to make a large investment in time and effort to obtain, and maintain, the designation. Faculty are becoming frustrated with the program; indeed, one of the original 7 CAEIAEs (Purdue) declined to renew their designation. The problems identified above spring both from the personal experience of the authors in creating and maintaining Centers of Excellence and from surveys of CAEIAE participants.

We believe the program is flawed. We believe, equally strongly, that the flaws can be remedied. The result will be a program more effective than the current one that meets or exceeds all of the goals of the program. Our purpose in writing this paper is to discuss the weaknesses of the program openly, and by bringing them out into the open, help the program sponsors create a truly effective, long-term, robust, and successful program.

The ideas in this paper are just one set of possible improvements. Others within the security community undoubtedly have equally valuable, or better, ideas. We welcome a discussion of them, and hope that others become involved in working towards improving the quality of the CAEIAE program.

VI. References

[1] Birney, A. "Secure Coding? BAH!", Editorial, InfoSecurity, Jan. 2004.5

[2] Bishop, M. "The State of INFOSEC Education in Academia: Present and Future Directions," Proceedings of the National Colloquium on Information System Security Education pp. 19–33 (Apr. 1997).

[3] Bishop, M. "Academia and Education in Information Security: Four Years Later," Proceedings of the Fourth National Colloquium on Information System Security Education (May 2000)

[4] CISSE. "Colloquium for Information Systems Security Education", http://cisse.info/colloquia/cisse1/intro.htm

[5] CSIA."Federal Funding for Cyber Security R & D", CSIA Alliance, July 2005, http://www.csialliance.org/CSIA_RD.pdf

[6] Dittrich, D. "Invasion Force", Information Security, Vol. 8.3, March 2005.

[7] McAffee, Top 10 Security Threats for 2008, http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_avert_predictions_2008.pdf

[8] NSA. IASP Program, http://www.defenselink.mil/cio-nii/sites/iasp/

[9] NSA, NSA IACE Courseware evaluation program, http://www.nsa.gov/ia/academic_outreach/iace_program/index.shtml

[10] NSA. "NSA Centers for Academic Excellence", http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

[11] NSA, CNSS Standards, http://www.nsa.gov/ia/academic_outreach/nat_cae/cae_iae_program_criteria.shtml

[12] NSF SFS Program, https://www.sfs.opm.gov/

[13] Spafford, E. "A Failure to Learn from the Past", ACSAC, 2003, http://www.acsac.org/2003/papers/classic-spafford2.pdf

[14] Task Force on ACM/IEEE Curriculum, Computing Curricula 2005 http://www.acm.org/education/curric_vols/CC2005-March06Final.pdf

[15] Taylor, C. and J. Alves-Foss, "The Need for Information Assurance Curriculum Standards", Proceedings of the 2005 CISSE, Atlanta, GA June 2005

[16] Taylor, C. and J. Alves-Foss, "An Academic Perspective on the CNSS Standards: A Survey", Proceedings of the 10th Colloquium for Information Systems Security Education, Adelphi, MD June 5-8, 2006

[17] Yasinac, A. and M. Burmester. "Centers of Academic Excellence: A Case Study", IEEE Security and Privacy, Vol. 3, 1, 2005

[18] M. Bishop, "Education in Information Security," IEEE Concurrency 8(4) pp. 4–8 (Oct. 2000).