Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

NSA/DHS CAE Application Lessons Learned

Thomas A. Augustine, Patrick Vincent, Donald M. Needham, *United States Naval Academy*

Abstract – Designation as a National Security Agency/Department of Homeland Security Center of Academic Excellence requires a campus wide commitment to information assurance curricula as well as a rigorous application process. This article describes one institution's lessons learned in the application process from initial decisions to apply though to final application submission.

Index terms – Lessons Learned, Center Academic Excellence, Cyber Security Center

I. Introduction

The National Security Agency (NSA) and Department of Homeland Security (DHS) jointly sponsor institutional designation as a Center of Academic Excellence, limited to those nationally or regionally accredited four-year undergraduate and graduate studies institutions meeting specific information assurance criteria. Such designation acknowledges an institution's commitment to providing credible information assurance education opportunities to its students, and requires external review through a rigorous application process. To date over 100 institutions have earned this designation, each with its own story about why they applied and the steps they took to achieve the designation. This paper focuses on the reasons for undertaking the application process, lessons learned and the institutional expectations behind the United States Naval Academy's application for designation as a Center of Academic Excellence in Information Assurance Education.

Thomas A. Augustine, D.CS is an Assistant Professor in the Computer Science Department at the United States Naval Academy. Thomas.augustine@hotmail.com

Patrick Vincent, Ph.D. is an Assistant Professor and the Associate Chair of the Computer Science Department at the United States Naval Academy. vincent@usna.edu

Donald M. Needham, Ph.D. is a Professor and the Chair of the Computer Science Department at the United States Naval Academy. needham@usna.edu

II. Center of Academic Excellence Application Process

Schweitzer, Humphries and Baird [1] detail the process for applying for institutional designation as a NSA/DHS Center of Academic Excellence in Information Assurance Education (CAE/IAE). This process includes a two-pronged approval. First, institutions must map their existing coursework to the National Training Standards for Information Systems Security (NTSISS). This involves elaborating on how an existing set of course curricula teaches hundreds of individual line-items as listed in these standards.

Once this course mapping is submitted and approved by a committee of evaluators, institutions may then submit their Application for CAE/IAE designation. This application consists of nine essay questions which help evaluators determine the institution's commitment to interdisciplinary studies in information assurance related subject matter.

One of the application areas deals with creating a center or focal point to enhance cyber security knowledge, curriculum advice and information dissemination. The application acceptance criteria allow a broad interpretation of the specific implementation and goals to be accomplished by the designated center.

III. A College-wide Cyber Security Focus

Over the past few years there has been an increased government, military and industry focus on protecting the National Cyber Infrastructure. With the announcement of the creation of the Department of Defense's United States Cyber Command, and the stated cyber security focus of the last two presidential administrations, the Academic Dean and Provost of the United States Naval Academy tasked a campus-wide, inter-disciplinary committee with exploring options to ensure that the Academy's program prepares graduates to meet the future cyber-security focused requirements of its primary government sponsors. This committee interviewed seven professors from Institutions designated as Center of Academic Excellence, staff members from across the Department of the Navy and analyzed cyber-focused strategy recommendations from the Departments of Defense and Navy. Ultimately,

this committee provided a number of recommendations to senior decision makers, including seeking institutional designation as a CAE/IAE and the creation of a Center for Cyber Security Studies to further facilitate an inter-disciplinary focus on cyber security.

IV. Benefits of Choosing CAE Designation

Many of the benefits of CAE/IAE designation are chronicled throughout the literature. Streff and Zhou [2] note that such designation benefits the National information assurance training pool, opens opportunities for National Science Foundation and Department of Defense grant opportunities, stimulates academic research opportunities and provides positive publicity for the institution. Frincke and Bishop [3] note that the CAE/IAE designation opens doors for further research and resources with academia, government and industry counterparts. Yasinsac and Burmester [4] credit the Department of Defense's Information Assurance Program and a similar National Science Foundation program as a primary reason for the success of their information assurance Programs. Attainment of CAE/IAE designation is an important milestone for institutions seeking to enhance information assurance related opportunities for their students.

At the United States Naval Academy, we found all of these arguments to be foundational to our own goals for seeking CAE/IAE designation. After gaining committee-wide concurrence that the CAE/IAE designation was an important next step in strengthening our focus on information assurance, we sought to tailor the tangible benefits of such designation for each stakeholder. Our faculty gain additional research opportunities and contacts with industry and government agencies. Although students at the United States Naval Academy are ineligible for additional scholarships, they are highly motivated to undertake internships and thereby also gain experience in working with industry and government agencies. The CAE/IAE designation provides a variety of avenues for such internships. While faculty and students are key stakeholders in the designation process, a commitment from the institution's administration and board of directors is necessary to ensure the longevity of such initiatives. In our case, the administration focused on how the CAE/IAE designation would assist the Academy in producing graduates with skills required by our primary employers, the United States Navy and Marine Corps.

V. Issues in Choosing CAE Designation

Through our interviews with other CAE/IAE designated institutions, we determined that each school has its own unique reasons for deciding when and whether to apply for designation. Common to all interviewed was a need to perform a cost-benefit analysis of any such undertaking. There are many certifications and designations that an institution can choose to pursue. Certainly regional or national accreditation of institutions and programs take precedence in resource allocation. In the case of the Naval Academy's computer science, information technology and 6 engineering programs, there is an institutional emphasis on maintaining national and international prominence through ABET accreditation, which can require a large amount of time, analysis and documentation throughout the school year.

In exploring the benefits of the CAE /IAE designation, we encountered many of the issues discussed by Bishop and Taylor [5]. First was skepticism of mapping our coursework to training standards instead of well vetted academic standards, created by consensus of academics. The academic community tends to govern through consortium, while the Government tends to certify through existing standards and regulations. While the NSA/DHS Center of Academic Excellence designation is purely voluntary, many of the institutions interviewed had to reassure faculty that this designation would not dictate a long-term change in curriculum, but in fact simply focused on certifying that the existing curriculum met or exceeded written standards.

Possibly the largest hurdle in applying for this designation is an understanding of the culture of the institution and striving to address the concerns of faculty. Bishop and Taylor discuss the differences between government and academic goals as noted in many surveys of CAE/IAE applicants [5]. Although we most likely had the factors necessary to become designated five or more years prior, we recognized the need to have the support of faculty and senior leadership which is best attained through a thoughtful review of the tangible benefits of receiving a government designation. Towards this end, we first sought to demonstrate that curriculum could be modified through the typical committee-driven academic process and would not be negatively impacted by applying for NSA/DHS designation. Over time this was directly demonstrated by fully designing and teaching the information assurance and networking curriculum to meet the needs of graduates and our primary ABET accreditation standing, as opposed to designing courses to meet a certification or designation criterion. We felt we were ready to proceed with CAE/IAE designation after having first obtained ABET, academic community, faculty and student feedback noting the strength of these programs.

An additional initial concern of some of the computer science faculty was the perception that a focus on cyber-security may change the overall focus of the department. Currently our Computer Science Department offers

rigorous ABET accredited programs in computer science and information technology, in which computer networking and information assurance represent only about 20 percent of the curriculum. Faculty rightly noted that our disciplines do not have a separate designation for computer programming, algorithms, architecture, databases or any of the other fields that we teach. By applying for and accepting a designation for information assurance excellence, institutions are implicitly agreeing to commit significant resources and time to the study of information assurance and cyber security. Thus, prior to applying, our faculty needed to ensure that the existing curricula and focus were strong enough to earn CAE/IAE designation while at the same time preserving the commitment to the ABET accreditation of the computer science and information technology programs.

Up to this point we have discussed the concerns primarily from the perspective of computer science faculty. Note that while information assurance is commonly thought of as a purely technical computer science or information technology field of study, the CAE/IAE application requires a campus-wide focus on information assurance subjects to include related technical fields, mathematics, foreign languages and culture as well as geo-political impact. Over the past year, the United States Naval Academy has benefited from steady growth in senior-leader support for a focus on cyber-security. Prior to this surge in support, the Computer Science department offered numerous courses in information assurance, cryptography, networking and digital forensics, while other departments including Political Science, Mathematics and Electrical Engineering offered courses in information security related fields such as national security policy, secure sockets, and biometrics respectively. While these courses were regularly offered to seniors in their respective majors, there was minimal emphasis on integrating these into a cohesive, multi-disciplinary program. After this increased leadership focus on cyber-security, the Naval Academy chose to create a Center for Cyber Security Studies. The CAE/IAE certification requires some type of center, but by creating this cross-disciplinary center at the dean's level with a full-time director, the college president, board of directors and senior deans gave faculty from multiple departments increased motivation to integrate cyber security efforts throughout the campus.

VI. Lessons Learned in Mapping Coursework

Every institution will have a different process to gain faculty and senior administration support in applying for the CAE/IAE designation. Some institutions will likely be able to gain this support immediately, while others may require a focused marketing campaign. Once a commitment to apply is made, there are a number of lessons learned that we have observed which can be useful to those creating a plan to apply in the future.

A. Develop and Implement a Repeatable IA Curriculum

Once an institution has made a commitment to apply for the CAE/IAE designation, a first step is in developing and implementing a strong, repeatable information assurance curriculum. We developed and refined a curriculum for the primary information assurance course complete with 30 hours of lecture and 30 hours of hands-on lab experiences. After offering the course to more than a dozen class sections, receiving positive feedback from the ABET accreditation evaluators, and sharing our course curriculum with multiple undergraduate institutions and government agencies, we were confident that the curriculum taught met or exceeded the requirements of the information assurance community. While an institution must map one or more of its courses against the National Training Standards for Information Systems Security (NTSISS) prior to applying for the CAE program, many institutions find it difficult to correlate training standards with educational concepts. We made a conscience effort to ensure that we educate students to think critically while combining their computer science and information technology skills rather than simply training students to administer existing security requirements. Though the NTSISS standards provide a strong outline for topics that make up the field of information assurance, they are not presented in a consolidated cohesive manner fit for direct course curriculum development. Had we simply mapped our information assurance courses to the NTSISS standards, rather than first develop coursework and later map the coursework to the standards, we may have lost opportunities to gain the synergy in teaching foundational computer science and information technology areas of study. Additionally, we gained support for the CAE/IAE designation from senior faculty and deans by noting that this designation would simply add an additional validation to an already strong program as opposed to simply chasing a certification or designation.

B. Understand the National Training Standards for Information Systems Security

The National Standards for Information Systems Security were created in 1994 by the Committee on National Security Systems, a consortium of primarily government agencies, in an attempt to codify the knowledge or skills required of information assurance professionals. As the only national standards available, the National Security Agency adopted these standards as the minimum areas to

be covered in information assurance programs. These standards were written to categorize government civilian and contractor training requirements, and the individual line item requirements were ordered accordingly. At first glance, these standards seem to duplicate individual line items. Upon further study, one notices that there are standards at both the awareness and performance levels. There is further decomposition by topical content as categorized by government definitions which directly correlate to a given syllabus. Unfortunately, this sample syllabus did not match our course curriculum as these standards were designed as documentation of training almost a decade before most colleges defined current best practices in information assurance education.

Before mapping our curriculum to these standards, we first re-categorized each line item based on our existing curriculum. In our curriculum, we first require networks and systems architecture courses as pre-requisites to an information assurance syllabus. We designed this course by starting at the outer edge of the network, working into operating systems, securing applications then discussing associated topics like cryptography, contingency planning and government/industry dependent concepts. Though this re-categorization did not produce a specific deliverable for the application process, it allowed us to group items which we felt correlated to specific areas of study, and that in turn allowed us to map multiple areas in the standards to a given week or subject matter in a course.

One such example of how this re-categorization helped us to consolidate many of the seemingly disparate areas of study follows:

Under NSTISS standard 4011, there are approximately 250 line items broken into awareness level and performance level concepts [6]. Awareness level categories include: Communications Basics, Automated AIS Basics, Security Basics, NTISS Basics, and System Operating Environment. Performance level categories include: NTISS Planning and Management, and NTISS Policies and procedures. Within each of these categories, subjects like confidentiality, integrity, and availability are listed in slightly different contexts.

Our first lesson and lab in our information assurance course deals with an information assurance model which elaborates on each of these topics. Instead of mapping our coursework to these standards, we took the opposite approach of mapping these standards to specific weeks or units within our curriculum. So while each of these topics is listed separately at least five times each in the standard, we had only to find it once, and then link it to the appropriate lesson and lab number. With over 250 items in the 4011 standard and 5500 items in the 4013 standard [7], we were able to significantly reduce the amount of time spent finding and listing course references by dozens of hours simply by grouping the standards to our curriculum instead of vice versa.

C. Map to the minimum number of courses

Through our dialog with the CAE/IAE designation program managers at NSA, they noted that many educational institutions believe they need to map multiple courses to show that they are involved in information assurance throughout their curriculum. The program managers noted that this is the purpose for the application documentation, not the course mapping to NTSISS standards. The purpose of this mapping is simply to demonstrate that an institution meets national standards for teaching the minimum information assurance subjects to some subset of the students at the institution. As such, they prefer the minimum number of courses mapped to these standards. Fewer courses imply that students are getting concentrated emphasis on this subject matter. They further note that if an institution must map all of these individual requirements to a large number (such as ten or more) courses, students are likely not receiving an in depth enough education in information assurance principles to designate an institution as a CAE/IAE.

After reviewing the standards, we chose to map all of the requirements for both the NSTISS 4011 – Information Security and NSTISS 4013 – System Administrators in Information Security using three courses [6, 7]. We mapped about eighty percent of all line items to our initial information assurance course. While we offer a number of information security related courses such as advanced information assurance, networking, advanced networking, cryptography and digital forensics, the majority of our students take the information assurance course, thus maximizing our potential to give our students the Committee on National Security Systems certification for coursework taken. In addition to information assurance, we mapped areas from our computer networks and computer architecture courses. Through these three courses we were able to map all 600+ line items to existing coursework. Given the standards initial intent to document training of government workers, there were a number of government specific line items that are not currently taught. Additionally, there are concepts like modem security which is no longer a focus in modern network information assurance courses. We did have to apply some adjustment to our information assurance course to map to the standards, adding some concepts to some lessons plans and an entire hour discussing government specific terms, policy and concepts.

Table 1 and Table 2 display statistical information for the mapping of our curriculum to 4011 and 4013 standards. These tables show that while the mapping of 4011

required three courses and mapping 4013 required only one course, these standards include only a subset of the overall curriculum taught. Through a well designed curriculum, we were able to address all of the knowledge required of the standards while reserving plenty of additional lectures and labs to meet the goals of our accreditation board, key stakeholders, faculty and students.

Courses used in mapping	3 Network/Architecture/IA
Total IA-related Lectures/Labs	80 Lectures/Labs
70% of standard mapped	10 Lectures/Labs
30% of standard mapped	18 Lecture/Labs
% Lab/Hands-on used in mapping	18
# Line Items in standard	261
# References to Courses	453

Table 1. NSTISSI-4011 Mapping

Courses used in mapping	1 Information Assurance
Total IA-related Lectures/Labs	60 Lectures/Labs
70% of standard mapped	13 Lectures/Labs
30% of standard mapped	27 Lecture/Labs
% Lab/Hands-on used in mapping	35
# Line Items in standard	578
# References to Courses	870

Table 2. NSTISSI-4013 Mapping

D. Use IA Course creators and coordinators to map to the standards

Mapping to the standards can be a tedious process. First, as noted, there can be hundreds of individual line items. Second, the online data entry user interface is very awkward and difficult to manipulate. We were initially tempted to "divide and conquer," giving a large number of individuals a smaller section. However after reviewing the standards, we chose to have the information assurance course coordinator take the lead, while asking our course coordinators for the computer architecture and computer networking courses to help answer specific questions. There are so many topics and duplicate responses when mapping these standards to courses that adding additional personnel would likely have served to confuse and duplicate the existing work load. In using the expertise of the information assurance course coordinator, we were able to much more easily determine how and where specific line items are taught. Though most of our staff would understand the concepts listed in the national standards, and would generally be able to look at syllabi and find major subject matters taught, mapping to these standards requires an in-depth understanding of how and when each subject is taught. Likewise, since twenty percent of the subjects were mapped to two different courses, we asked the other course coordinators to fill in their areas after the information assurance instructor verified that these areas were prerequisites to the information assurance course.

This method reduces confusion and duplication of efforts but does demand a large time commitment from the primary individual mapping the coursework. Unfortunately, populating the submission database requires a large administrative burden as we had almost 1000 line items, each requiring navigating through many hyperlinks. We chose to ask the knowledge area experts to both determine how each line item should be answered and place the information in the database. Had we planned for the difficult navigation through the database, we may have asked the knowledge experts to record their information differently to allow administrative staff to process the data.

D. Plan for a Compressed Timeframe

Relatively few people can be involved in the course mapping process. These individuals also tend to be key instructors and course coordinators making the mapping process not only tedious but very time dependent as well. We started mapping our courses at the end of August, during the start of the semester. It took us almost one hundred hours to understand the process, add the data to the database and validate the course mapping process. Knowing that these individuals would also likely be involved in the CAE/IAE application, and understanding that it can take the evaluators weeks to give feedback on the mapping, we chose to have our mapping completed by mid October. While we completed this process on time, we recommend designating this as a primary duty during the semester proceeding the semester of application, and/or reducing the courses taught or otherwise factoring in this additional workload as appropriate for the institution.

VII. Lessons Learned in CAE Application

After obtaining certification of coursework in accordance with CNSS standards, an institution is then invited to apply for designation as a CAE/IAE. We found this process considerably easier than mapping the coursework. Unlike mapping the coursework, this portion could be easily split among faculty with a minimum time or administrative burden. This application consists of nine essay questions which can be answered fairly easily if an institution has a well established information assurance program with additional faculty and course offerings from outside the department primarily overseeing information assurance education, the Computer Science Department in our case.

A. Gain Senior-level Support Prior to Applying

We found that a few individuals can not successfully advocate for CAE/IAE designation on their own. Rather, the chair of at least one department must market the benefits of this designation to his or her department, and after receiving that level of support, must further advocate benefits with other departments. Our experience shows that once multiple departments or functional areas understand the likely benefits associated with institutional designation, the institution's deans and senior leaders can move forward and add the necessary focus to their strategic goals for the institution.

By gaining support and having multiple departments push for designation and creation of a center to integrate these efforts, we were able to maximize faculty, senior leader and student interest in information assurance related subjects and activities. Additionally, by demonstrating a strong program prior to applying, we were able to gain support from our board of directors and alumni association thereby furthering information assurance interest in both faculty research and student activities.

B. Demonstrate Funding Opportunities in Information Assurance before Applying

Over the past four years, we have actively solicited research, equipment and student activity funding from various government agencies used primarily in information assurance areas of study. Through this funding we have been able to provide multi-disciplinary opportunities for both faculty and students. In describing the benefits of CAE designation, we were able to capitalize on support from those who benefitted from our funding efforts. This support resulted in faculty motivation to offer courses in information assurance outside the computer science department, a key component in the CAE/IAE application process.

C. Assemble a Multi-Disciplinary Team of Experts

While it is possible to answer the nine questions for the CAE/IAE application with a single, knowledgeable person, we chose to setup a team of cyber-security interested faculty and staff in a committee chartered by the Academic Dean and Provost. This committee made a number of recommendations to senior leadership including application for CAE/IAE designation. These recommendations were made only after discussing the benefits to the Academy, faculty and students as well as interviewing members from government, industry and academia. Through this process of consensus and process ownership, we were able to greatly enhance faculty and senior administration support for the CAE/IAE application process.

D. Interview CAE/IAE Designated Institutions and NSA/DHS CAE Program Directors

After deciding to apply for CAE/IAE designation, we contacted seven CAE/IAE designated institutions and interviewed those involved in the application or re-designation process. We chose institutions that were either similar to our institution, had experts with nationally recognized experience in information assurance education or those graduate programs for which we commonly send our students after graduation. These institutions included: the United States Air Force Academy, United States Military Academy, Mississippi State, University of Tulsa, Air Force Institute of Technology, Naval Postgraduate School, and Johns Hopkins University. Each institution contacted readily provided us with detailed lessons learned which were invaluable to our process.

These lessons learned saved us time, clarified the application process and helped us focus our efforts. Many of the lessons learned described in this paper were a result of these discussions. In addition to lessons learned many of these institutions provided us sample copies of their applications. While each institution has a different program with separate strengths and constraints, comparing the application wording from other successful programs allowed us to better tailor our application.

E. Set Up a Website for Support Information

A great deal of supporting information is necessary throughout both the NSTISS course mapping and CAE/IAE application process. The course mappings require course syllabi and policy statements, as well as examples of presentation and lab experiences. Evaluators of the CAE application are further required to verify specific documentation listed in each of the nine questions of the application. While writing the application multiple faculty members must provide documentation. The input database limits file size and format to text and hyperlinks only. By setting up a password protected website, we were able to provide dozens of links to supporting documentation visible to all application writers and evaluators in the desired format. By setting credentials for these sites, we were able to post supporting information including institution proprietary information, student work and course assessment data. Setting up a website provided a single, consolidated location for all application related data and streamlined our information delivery.

F. Understand that Information Assurance is a Broad set of Topics

Perhaps the best advice we received came from Dr. Ray Vaughn of Mississippi State University when he encouraged us to keep in mind that information assurance encompasses a broad set of topics. Resources such as NSTISS standards and the Certified Information Systems Professional Official Guide list many topics making up the field of information assurance [6,7,8]. For example, when application questions ask an institution to define its information assurance program, our initial focus was primarily on network security. Although an integral part of information assurance, network security is but one of dozens of topics associated with the study. By broadening our scope and including numerous fields, we were able to define a very strong multi-disciplinary program in information assurance, ultimately making our application much stronger.

This broader view of information assurance also helped us to better define the mission of our newly created Center for Cyber Security Studies. When addressing the need for a center, our faculty and administration initially asked how network security related to the many disciplines that would be a part of the center. However after addressing the many facets of information assurance to include topics such as physical security, cryptography, national policy and business continuity planning, faculty from many disciplines understood their role in information assurance as well as the need to integrate these studies under a single center.

G. Understand that the Entire Institution is being Evaluated

The NSA/DHS designation certifies that an entire institution's information assurance program meets or exceeds given standards. Since specific departments or disciplines are not given this designation, it is crucial to demonstrate that the institution regards information assurance as an important focus area.

Since we had full institutional level faculty and administration support prior to applying for the CAE/IAE, we were encouraged to use institutional wide resources in answering the application questions. About thirty percent of the application requires institutional level action including: outreach and collaboration agreements with other minority or technical colleges, institutional level information systems security practices and institutional access to information assurance resources. Another fifty percent of the application requires information about multi-disciplinary programs, faculty qualification and curriculum focused on information assurance. Without the approval and focus from our administration, we would have been unable to appropriately answer these institution-wide questions.

H. Review the Submission with Experts and Novices

Prior to submission of both the course mapping and CAE/IAE application, we invited both information assurance experts and novices to review, comment and strengthen the submissions. Although program managers will work with an institution to clarify statements submitted, the CAE/IAE submission must stand on its own, be fully documented and understandable by the evaluation committee.

Because we only had one opportunity to submit the CAE application without additional clarification or revision, we asked those experts close to the process to review the documentation for accuracy. We asked each reviewer to open every link to supporting documentation and verify that the correct content appeared in multiple web browsers. This process ensured that our application evaluators would be able to find all of the listed documentation.

Conversely, we also chose to invite a few information assurance novices to review the documentation to ensure no subject matter or institutional operating procedures were assumed. While we also asked these individuals to verify the accuracy of documentation, we further asked them to determine whether they felt that the wording and supporting documentation answered the various questions. Despite our prior 'expert' validation, we were nonetheless able to receive valuable feedback from our novices.

VIII. SUMMARY

Though the process for mapping courses to standards and applying for the NSA/DHS Center of Academic Excellence in Information Assurance Education designation is well documented, each institution must define its own reason for applying, gain faculty and administration support and document its program. We defined a number of lessons learned in applying for designation.

Prior to applying for designation we first created an information assurance curriculum founded on strong principles and lab experiences.

Key among lessons learned prior to application is an institutional commitment from both multi-disciplinary faculty and senior administration for a strong information assurance program and focus. We chose to gain this support by forming a multi-disciplinary committee to provide recommendations for all of our campus-wide

information assurance courses and priorities. This approach helped us to gain valuable support and buy-in from both faculty in many departments and our senior administration.

Finally, there is a large administrative burden associated with mapping information assurance courses to NSTISS standards and filing the CAE/IAE designation application. Additionally, there are many factors that effect successful application and subsequent designation as a CAE/IAE. We were able to gain valuable insights into these processes by interviewing experts from many institutions and applying their lessons learned to our application process.

Through the lessons learned gained from our fellow institutions, many of which were documented in this paper, we were able to successfully navigate obstacles and define best practices in applying for an NSA/DHS Center of Academic Excellence.

IX. References

[1] D. Schweitzer, J. Humphries, L. Baird, "Meeting the Criteria for Center of Academic Excellence (CAE) in Information Assurance Education", Journal of Computing Sciences in Colleges, Vol 22, Issue 1, 2006, pg 151-160.

[2] K. Streff and Z. Zhou, "Developing and Enhancing a Computer and Network Security Curriculum", Journal of Computing Sciences in Colleges, Vol 21, Issue 3, Feb 2006, Pg 4-18.

[3] D. Frincke and M. Bishop, "Joining the Security Education Community", IEEE Security and Privacy, Vol 2, Issue 5, 2004, pg 61-63

[4] A. Yasinsac and M. Burmester, "Center of Academic Excellence: A Case Study", IEEE Security and Privacy, Vol 3, Issue 1, 2005 pg 62-65.

[5] M. Bishop, and C. Taylor, "A Critical Analysis of the Centers of Academic Excellence Program", *Proceedings of the 13th Colloquium for Information Systems Security Education*, Seattle, WA, Jun 2009.

[6] NSTISSI-4011 - INFOSEC Professionals, National Training Standard, 1994.

[7] NSTISSI-4013 - System Administrators in Information Systems Security, National Training Standard, 2004.

[8] S. Hansche, J. Berti, and C. Hare, Official ISC2 Guide to the CISSP Exam, CRC Press LLC, 2004.