National Center of Academic Excellence in Cyber Security and Information Assurance. An Implementation Case at Cameron University

Pedro A. Diaz-Gomez\(^1\), Mike Estep\(^1\), Johnny Carroll\(^1\), and Reza Kamali\(^2\)
\(^1\)Computing & Technology Department, Cameron University, Lawton, OK, USA
\(^2\)College of Natural Sciences, California State University at Stanislaus, Turlock, CA, USA

Abstract—The goal of this paper is to present the experience of the implementation of a Center of Academic Excellence in Cyber Security and Information Assurance, in order to share the experience with the academic community, pretending to help future implementations of Centers of Academic Excellence following the guidelines of the National Security Agency.

Keywords: accreditation, certification, cyber security, information assurance, information security.

1. Introduction

The Department of Computing & Technology at Cameron University (CU), proposed the creation of a Center of Academic Excellence (CAE) in Cyber Security and Information Assurance in September 2010, with a three years goal of implementation, using the synergy of the Cyber Security Education Consortium (CSEC), which is a National Science Foundation of advanced technological education, dedicated to building an information security workforce who will play a critical role in implementing the National strategy to secure cyberspace.

The requirements to become a Center of Academic Excellence help the IT program to pursue its goal, the University Mission and University Plan 2013: the Center of Academic Excellence, as its name implies, will provide to students access to quality educational opportunities, experiential learning, will prepare them for professional success, responsible citizenship and meaningful contributors to the priorities of our Nation [1].

The University core values of excellence in teaching, scholarship, service, and mentoring; leadership in our community and region, forming partnerships and collaborative relationships, as well as serving the community and region by sharing our expertise; the goals of building distinction in the area of Information Technology, of strengthen partnerships with Fort Sill to provide educational opportunities for soldiers, and of increasing educational partnerships with career technology centers and community colleges, will be part of our requirements for becoming a Center of Academic Excellence [1]. This is a great opportunity to fulfill the University mission and to work toward the accomplishment of the CU strategic plan 2013 (more information on CU strategic plan can be found at [1]).

2. Requirements

The National Centers of Academic Excellence are granted to two years programs in Information Assurance (CAE2Y), and four year institutions in Information Assurance Education (CAE/IAE). A letter of intent must be send to the NSA stating the desire to apply for the CAE program, verifying status as a 2-year institution—for the CAE2Y—,
and providing evidence of national or regional accreditation. The letter of intent must be on official institution letterhead, signed at an appropriate level (Dean or higher), and mailed to the NSA Program Office prior to the due date for the CAE application.

As a prerequisite the courseware must be certified under the Information Assurance (IA) Courseware Evaluation Program as meeting the Committee on National Security Systems (CNSS) Training Standard [2]. The CNSS Training Standard 4011 is required and at least one additional CNSS Training Standard (4012, 4013, 4014, 4015, 4016 or subsequent standards) is required.

The NSA additionally requires six criteria for the CAE2Y and nine criteria for the CAE/IAE which will be detailed in Section 2.2.

2.1 CNSS Certifications

As stated in section 2 one prerequisite for getting the National Center of Academic Excellence is to meet at least two training standards from the CNSS including the National Training Standard for Information Systems Security (INFOSEC) Professionals NSTISSI-4011 which includes the minimum course content for the training of INFOSEC professionals in the disciplines of telecommunications security and automated information systems security [2]. At least other CNSS Instruction must be chosen from the CNSSI-4012 National Information Assurance Training Standard for Senior Systems Managers, the CNSSI-4013 National Information Assurance Training Standard for System Administrators, CNSSI-4014 Information Assurance Training Standard for Information Systems Security Officers, CNSSI-4015 National Training Standard for Systems Certifiers, CNSSI-4016 National Information Assurance Training Standard for Risk Analysis, or a subsequent standards [2].

2.2 NSA Criteria

The requirements that the Computing & Technology (CaT) Department must meet to become a CAE in Information Assurance Education (CAE/IAE) or a CAE in Research (CAE-R) are dictated by the NSA/Central Security Service and the DHS. Such CAE status is granted for a period of five years, after which we have to reapply in order to retain the designation.

The National CAE in Information Assurance may be granted to two years programs (CAE2Y) and four year programs (CAE/IAE). Since CU has a 2 +2 program in Information Technology (IT) with an option in Cyber Security and Information Assurance, CU is eligible to apply for both. The current plan is to meet the CAE2Y requirements initially and then meet the more substantial CAE/IAE requirements in the following two years.

To meet the requirements of the CAE2Y, an Institution must meet and provide evidence of having met each of the following requirements:

- IA Partnerships evidence must be in the form of an articulation agreement.
- IA Student Development Web site list degrees and IA curriculum with course description.
- IA as multidisciplinary subject IA incorporated in various disciplines.
- IA Outreach Strong collaboration with business, industry, government, and local community.
- IA Faculty assigned specifically to teach and/or develop IA courses/curricula/modules.
- Practice of IA encouraged throughout the Institution - The academic program demonstrates how the institution encourages the practice of IA, not merely that IA is taught.

There are nine requirements for the CAE/IAE. These nine requirements subsume the six for the CAE2Y, so as we accomplish the CAE2Y requirements:

- Outreach/Collaboration.
- IA treated as a Multidisciplinary Science.
- University Encourages the Practice of IA.
- Academic Program Encourages Student Research in IA.
- Faculty Active in Current IA Practice and Research.
- IA Resources.
- IA Academic Programs is Robust and Active.
- Declared Center for IA Education.
- Number of IA Faculty and Course Load.

The system used by the NSA to decide if the requirements are met involves a point system. Points are given for meeting various goals and when the required total points have been reached, the CAE is awarded (See [4]). For example, an articulation agreement with a community college is worth points as is an external speaker coming to campus to discuss Cyber Security issues. CU has already been working toward these goals and has already amassed significant points but there are yet significant points to obtain before the CAE are awarded.

3. Cameron University Implementation Plan

The six requirements of the CAE2Y are embedded in some of the nine requirements of the CAE/IAE (See Section 2.2). This suggest the general plan of working for getting first the CAE2Y that will benefit initially the student body that is pursuing the AAS, and after getting the CAE2Y, apply for the CAE/IAE that will benefit students in the BS program.

After some discussion, the CaT Department at CU decided that pursuit of a CAE with a target completion time of three years would be in the best interest of the department in spite of the fact that it is a very large undertaking. The Chair and lead faculty immediately started moving forward with the planning and, so far, CaT has been relatively successful overcoming obstacles.
The implementation of the goal to create a CAE at CU heavily involves utilizing the resources provided by the Cyber Security Educational Consortium. The goals of CSEC involve building an information security workforce who will play a critical role in implementing the national strategy to secure cyberspace. Synergies with and resources provided by CSEC are critical to the implementation of a CAE at CU.

The CaT Department is currently working on mapping the CNSS standards 4011 and 4012 to the actual curricula; in articulation agreements with Great Plains Technology Center and Rose State College, reaching out to the community especially at Ft. Sill, incorporating IA and Cyber Security into all of our various programs, developing multiple faculty in the IA area, beginning to work on a web site in support of our Cyber Security and IA programs, and organizing more external speakers to speak to our students and the Cameron community. Success in any one of these items will award us points to be applied to our CAE pursuit. It will take quite a bit of success to achieve our final goals.

3.1 CNSS 4011 and 4012 Course Mapping

The IT program has a common core that includes the following courses: Intro to Computer Information Systems, Intro to Networking, Programming Logic, Intro to Information Assurance/Security, and Fundamentals of Systems Analysis and Design. The program also includes three specialized options: Computer Information Systems, Management Information Systems, and Cyber Security and Information Assurance. The third option was chosen for integration of CNSS 4011 and 4012 course mapping, due to the inclusion of five related courses: Computer Forensics, Information Assurance Networking Fundamentals, E-commerce and Web Security, Security Architecture and Design, and Current Topics in Information Assurance and Network Security.

As the primary goal of the CaT Department was to pursue the CAE2Y, courses chosen for mapping were those taken by students in the AAS degree program. The majority of CNSS 4011 content was already covered in Intro to Information Assurance/Security. However, mapping curriculum for that course to CNSS 4011 helped to ensure a relevant textbook would be adopted, and that support content would be included in Intro to Computer Information Systems, Intro to Networking, and Computer Forensics. Mapping of CNSS 4012 was assigned in the Security Architecture and Design course (See Section 4).

Faculty training was a key component as well. At the beginning of the program, there was only one faculty member responsible for the Cyber Security and Information Assurance option. Currently, there are three faculty members that have received training with support of the Cyber Security Education Consortium and Cameron University. Five core areas proposed by CSEC were part of the training, as well as more specialized training courses in Intrusion Detection Systems, Penetration Testing, and Operating Systems Hardening. As a result of this training, faculty members began to pursue certifications.

3.2 Resources

For the CAE in Information Assurance Education to be successful, it will require CU to provide at least a minimal amount of resources. This includes faculty and staff resources and the use of space and equipment for labs.

A significant amount of the lab facilities are already available. Since the CAE will support the CaT Department and the Information Technology degree programs, funds from what was previously called the Brain Gain Grant are eligible to be used for equipment purchases. Also, it is planned for significant funding to be received via our relationship with CSEC. We believe that we will not need a large infusion of university funds to create required labs, but some funding may be required, especially for maintenance of those labs.

The CaT Department will request that CU provides 1/2 time release for the Director of the CAE. The staffing request will also include secretarial support and the support of a web/computer/network technician. It is possible that the technician resource can be filled by senior students in IT fulfilling the requirements of an internship.

Initially, the Director will have the responsibility to oversee the pursuit of the fulfillment of the criteria needed for being a CAE. After CU has been awarded the CAE, the responsibility will include the maintenance of such criteria in order to reapply for accreditation when needed. This task will involve keeping the cyber security and information assurance option syllabi up to date, faculty properly trained in bleeding edge Cyber Security issues, partnerships and program agreements, student development, information assurance outreach, research, and publicity. Also, once the CAE2Y is obtained, the director will be responsible for ensuring that the department moves reasonably quickly toward the baccalaureate level CAE/IAE.

Part time secretarial/receptionist support is also requested. This secretary/receptionist will answer the phone, make appointments, and similar activities along with other duties such as typing and filing.

The support of a technician is also requested. The technician would assist the director and faculty in the upkeep of the Cyber Security labs including the computers, networks, and etc. It is also hoped that the technician would be able to maintain the Cyber Security web site. It is possible that we could use one or more student interns to fulfill this role.

A budget specifying previous resources was elaborated.

4. Student Perceptions

In the fall of 2011, the Cameron University Department of Computing and Technology course IAS 3263 Security Architecture and Design was structured with a focus of
including CNSSI 4012 elements in the curriculum. The students were made aware of this in the course syllabus and by the instructor. Discussions also ensued on the possibility of the department working toward becoming an NSA Center of Academic Excellence. In a course assignment, students were given the task of conducting research on CNSSI 4012 and Academic Center of Excellence guidelines. They then had to provide their perceptions, related to possible implementation in the course and in the department. Below are a few of the student responses taken from the assignment.

- Overall, accreditation from the NSA is something that should be highly sought after — the accreditation means that the university is able to provide a wide range of information and resources dealing with IA, while still holding the guidelines that are used by professionals in the workplace. On top of that, the centers that are accredited, are also considered models for the nation, in terms of education of IA.
- Following research of this topic, I have come to learn that becoming a Center of Academic Excellence is a top priority of the Department of Computing and Technology, as well it should be. This program was set up by various government agencies in order to educate and train the next generation of network security administrators to protect our country from foreign cyber threats. The importance of this training could give our country the upper hand in any conflict. Being able to protect important information about our military, government, and economy is of the utmost importance and should not be taken lightly.
- From my experience so far at Cameron University, most of our assignments are writing papers, which is good, but a lot of times I feel like we should be doing more practical assignments to better understand how what we read can be applied in the real world. With that said, we can be given information security case scenarios, and then use the guidelines from CNSSI 4012 to address the issues. For example, CNSSI 4012 comprises of ten functions. A scenario can be given in which network vulnerabilities have been found, and we would have to refer to function ten (assess network security) to address the issue.
- Based on the functions which are similar to IAS 3263, some possible ways that the CNSSI 4012 can be used in this IAS 3263 course are: furthering awareness and knowledge of countermeasures, defenselessness or vulnerability with security systems, risk management and policy direction, acquisition and life cycle management, assigned responsibilities, allocation of resources, and others. These areas can be addressed and explained in more detail, so that new IA professionals can be better equipped in outside workplace settings to help improve systems infrastructures.

The authors believe student understanding and perception to be an important factor to consider in becoming a Center of Academic Excellence. This particular exercise in IAS 3263 also seems to have helped the students to take ownership of their cyber security education, while providing a sense of realism beyond the classroom.

5. Conclusions and Future Work

This paper presented the process of the creation of a Center of Academic Excellence in Cyber Security and Information Assurance at Cameron University, as an experience that can be taken by other Institutions in their pursuit of excellence. A CAE will help Departments in their efforts to fulfill standards in IA that will benefit academia in general and Students in particular. In the case of Cameron University, the CAE will help it solidify its position as the University of Choice by attracting high-quality students. These students will benefit from the high quality of teaching provided by outstanding faculty accompanied by significant opportunities for experiential learning. Students will have the opportunity to receive significant scholarship funding from the DoD and other government scholarship programs. Finally, the department will reach out to the community creating new partnerships with technology centers, other colleges, and forge and/or cement partnerships with the industrial community including the local military industrial complex and local companies.

It is the opinion of the CaT Department that the creation of the proposed CAE in Cyber Security and Information Assurance would be a very positive step for Cameron and be very beneficial to the university, the faculty, and to the students. This is a great opportunity to fulfill the University mission and to work toward accomplishing the goals of the CU’s strategic plan 2013.

References


