UNIVERSITY OF
SOUTHERN MAINE

University of Southern Maine

USM Digital Commons

Faculty Publications   **Philosophy**

2015

Experiences with Establishment of a Multi-University Center of Academic Excellence in Information Assurance/Cyber Defense

Julien Murphy PhD
University of Southern Maine, jmurphy@maine.edu

R.T. Albert
University of Maine at Fort Kent

C. Bennett
University of Maine at Farmington

David Briggs PhD
University of Southern Maine, briggs@maine.edu

Maureen Ebben PhD
University of Southern Maine, maureen.ebben@maine.edu

See next page for additional authors

Follow this and additional works at: https://digitalcommons.usm.maine.edu/philosophy-faculty

Authors

Julien Murphy PhD, R.T. Albert, C. Bennett, David Briggs PhD, Maureen Ebben PhD, H. Felch, D. Kokoska, L. Lovewell, C. MacDonald, G. Markowsky, L. Markowsky, Edward Sihler, and G. Wilson

Experiences with Establishment of a Multi-University Center of Academic Excellence in Information Assurance/Cyber Defense

R. T. Albert[1], C. Bennett[2], D. Briggs[3], M. Ebben[4], H. Felch[5], D. Kokoska[5], L. Lovewell[6], C. MacDonald[6], G. Markowsky[7], L. Markowsky[7], J. Murphy[8], E. Sihler[6], G. Wilson[9]
[1]Arts & Sciences Division, University of Maine at Fort Kent, Fort Kent, ME, USA
[2]Division of Mathematics and Computer Science, University of Maine at Farmington, Farmington, ME, USA
[3]Department of Computer Science, University of Southern Maine, Portland, ME, USA
[4]Communication and Media Studies Department, University of Southern Maine, Portland, ME, USA
[5]Computer Information Systems Department, University of Maine at Augusta, Augusta, ME, USA
[6]Maine Cyber Security Cluster, University of Southern Maine, Portland, ME, USA
[7]School of Computing and Information Science, University of Maine, Orono, ME, USA
[8]Philosophy Department, University of Southern Maine, Portland, ME, USA
[9]Department of Technology, University of Southern Maine, Portland, ME, USA

Abstract – *The National Security Agency (NSA) and Department of Homeland Security (DHS), in response to an unmet workforce need for cybersecurity program graduates, jointly sponsor a program by which a post-secondary education institution may achieve recognition as a Center of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD). The program identifies standards, criteria, and an evaluation process. Many individual institutions have achieved recognition. The University of Maine System, composed of seven universities, is the first multi-university entity to achieve the CAE IA/CD recognition. The purpose of this paper is to share the key challenges, opportunities, and experiences that contributed to this achievement, and offer recommendations.*

Keywords: Cybersecurity, Information Assurance, Education, Collaboration, NSA

1 Introduction

Concerns over the unmet workforce need for cybersecurity program graduates continue as they have for the past few decades. Much effort has been expended to raise student awareness and interest in cybersecurity education. For example, progress has been made in the establishment of cybersecurity competitions that have stimulated interest.

Similarly, much progress has been made to improve the quality and consistency of post-secondary education through efforts such as the National Security Agency (NSA)/Department of Homeland Security (DHS) jointly sponsored National Centers of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) programs. One can argue that the NSA/DHS CAE IA/CD recognition program is serving as a de facto accreditation standard for the fledgling cybersecurity discipline.

The public University of Maine System (UMS) is comprised of seven, highly geographically dispersed universities, not one of which could generate adequate evidence to garner NSA/DHS CAE IA/CD recognition. Many factors, most of which are present in other public university systems in the nation, contributed to establishing a context ripe for change that ultimately led to the UMS achieving NSA/DHS recognition as the first *multi-university shared/distributed* CAE IA/CD.

The aim of this paper is to share the key challenges, opportunities, and experiences that contributed to this achievement, and offer recommendations for harnessing the potential synergy resulting from direct engagement in mutually rewarding collaboration and cooperation to achieve significant gains in preparing the future cybersecurity workforce.

2 Constituents

2.1 NSA/DHS

The NSA/DHS, in response to an unmet workforce need for cybersecurity program graduates, jointly sponsor a program by which a post-secondary education institution may achieve recognition as a CAE IA/CD. The goal of the NSA/DHS CAE IA/CD education programs is to "reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. " [1]

Recognized education program categories include two-year programs (CAE2Y), four-year programs (CAE IA/CD), and research focused programs (CAE-R). Designation by the NSA/DHS is valid for five academic years, after which the institution must successfully reapply in order to retain its designation.

"Applicants must clearly demonstrate, in sufficient detail, how they meet each of the program criteria and include supporting documentation where required and appropriate. Minimum requirements must be met for each of the ten criteria." [2]

The review and selection procedures indicate, "Qualified IA professionals from the National Security Agency, the Department of Homeland Security, and other government and academic partners will assess applications. Other qualified individuals will be invited to assess applications as needed." [2]

"…Applications for CAE IA/CD will be rated independently, using system identified in the criteria. Two reviewers will assess each application. If the two reviews are not in agreement, a third reviewer will be assigned. The program office will make a final determination based on all three assessments. The burden is on the Institution to clearly demonstrate their qualifications for the CAE IA/CD program." [2]

"The National IA Education and Training Program (NIETP) operates under national authority as the national manager for IA education and training relating to national security systems. Its programs, including the National Centers of Academic Excellence (CAE), assure the very finest preparation of professionals entrusted with securing our critical information."[3]

NIETP provides specific guidance for preparing an application and an online application submission website. Applicants are required to map their institution's curriculum to an established standard consisting of a framework of knowledge units and student learning outcomes.

CAE IA/CD requirements and evaluation criteria specifically related to inter-institution cooperation and collaboration include:

- *Outreach/Collaboration.* The institution must demonstrate how IA/CD is extended beyond the normal boundaries of the Institution.

  o Shared Curriculum or shared faculty (NSA CAE IA/CD Criterion 1a)
  o CAE Collaboration (NSA CAE IA/CD Criterion 1d) Partner in research/shared classes or shared events with other institutions. Institutions are encouraged to partner with other CAEs on cyber or IA/CD research/instruction.

- *Number of IA/CD/Cybersecurity faculty and course load* (NSA CAE IA/CD Criterion 7c).

2.2   University of Maine System

The UMS is "the state's largest educational enterprise with nearly 40,000 students of all ages enrolled in our seven universities, law school, and eight outreach centers located across the state." [4] Figure 1 illustrates the significant geographic dispersion of the universities comprising the UMS.
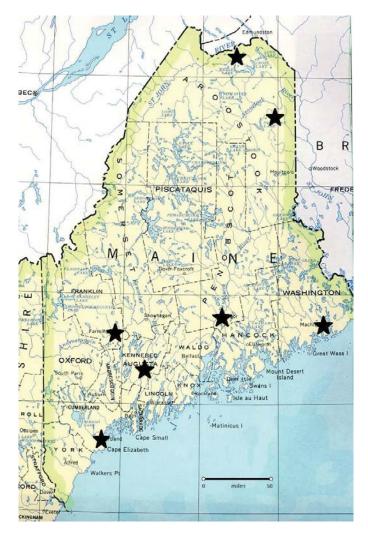

Figure 1. University of Maine System

A president who is accountable to the UMS Chancellor who, in turn, is accountable to a 16 member Board of Trustees (BoT) leads each university of the UMS. BoT members are appointed by the Governor and approved by the Maine Legislature for a five-year term.

In 2012-13, the Maine Cyber Security Cluster (MCSC) was funded by the Maine Technology Institute and the Maine Economic Improvement Fund to provide workforce and economic development initiatives across the state of Maine. Both the Executive Board and the Technical Advisory Board members were asked to fill roles on mission-critical subcommittees. These committees were comprised of business and industry, government, and military leaders in the cybersecurity, computer science, and information technology

sectors across the state of Maine, and selected faculty and staff of the UMS. An essential component of MCSC's mission is to create public-private partnerships and to build and support a collaborative environment among all interested and qualified parties.

Among the first MCSC subcommittees constituted was the Curriculum Subcommittee. This subcommittee was, agreed by all, to be extremely important to the educational and curricular mission of MCSC and to the Research and Development and Commercialization initiatives. Its efforts focus primarily on the design of a rigorous, appropriate, and topical student-oriented and knowledge unit based curriculum. The goals of Subcommittee were broadly stated: (1) attract strong students to the field of cyber security, (2) provide excellent training to students associated with MCSC, (3) develop programs that span the needs of the traditional university student and the wider community.

Curriculum development occurred in concert with the submission of the application for NSA recognition of the UMS as a CAE IA/CD. These two initiatives were pursued by a highly qualified and dedicated team of UMS faculty and staff.

2.3 ACM/IEEE

The Association of Computing Machinery (ACM) and Institute of Electrical and Electronic Engineers (IEEE) [5], though not yet playing a direct role in cybersecurity program accreditation, acknowledge the role of collaboration among faculty, educational institutions, business and government entities to build an "improved pipeline for a cybersecurity workforce" (p.4). Additionally, acknowledgement of barriers to such collaboration is exemplified through recognition that "academic departments are notoriously self-contained and reluctant to share resources, impeding collaboration and integration" (p.7). These are but two factors that influence inter-institution collaboration and cooperation.

3 Key Challenges and Opportunities

The challenges and opportunities that most significantly influenced this achievement arose from a geographic, governmental, and administrative context ripe for change. Collaboration and cooperation are key factors from which these challenges and opportunities arose. These factors have been widely cited in efforts to address cybersecurity from a multi-disciplinary approach [6], overcome barriers associated with academic silos [6], develop a strategy for fostering a shared understanding of concepts, guiding principles, and messages [7], and to improve the effectiveness of instructional methods [8].

Maine is often characterized as being a predominantly rural state with a widely geographically distributed public university system. The significant distances that exist between UMS universities presents challenges to inter-university communication and in turn inter-university collaboration and

cooperation. Poor driving conditions, often due to winter weather, have also contributed to impeding efforts to engage in face-to-face meetings. Technology has provided a means to attenuate such communication impediments however, progress on inter-university efforts is often retarded by such physical separation

The governmental landscape of Maine, specifically relating to post-secondary education, has been significantly influenced by Governor-led efforts and tension resulting from increased fiscal pressure. Among the casualties of such tensions has been the resignation of the Maine Community College President, demanded by the Governor, because he "… has not acted on some of his requests…" [9] The Governor's proposed budgets during his tenure have called for flat funding or very modest acknowledgement of requested funding. This has led to public cries and legislative action for much greater investment in higher education as a means to spur the state's economy toward greater prosperity through appropriate preparation of a highly skilled workforce. As with most other states in the nation, such fiscal pressures at the governmental level have steadily increased during the period of recovery from the most recent economic recession.

Regarding the administrative context, there have been several events, which in totality, presented key opportunities and an environment receptive to change. Among these are the UMS Mission Excellence campaign that was established in January 2012 by the UMS Board of Trustees (BoT).

> *"Mission excellence* is our term for a comprehensive process to sharpen our focus on our mission and bring increased value to our constituents. It means focusing our scarce resources and ensuring that our systems, structures, processes, and employees are as efficient and effective as they can be. Mission excellence is about creating an environment where faculty and staff are engaged in serving our constituents to the best of our abilities, where decision-making is done as close to the clients as competencies allow. In short, it is about being "best in class."[10]

One of the key aims of the UMS BoT during its development of the *Mission Excellence* goals and actions was to engage in "cost control" efforts to help avert a significant structural budget gap identified by the UMS BoT relating to increased cooperation and collaboration include forming additional business partnerships and collaborations (Directive II.a) and aligning academic and certificate program development with workforce needs (Directive II.b) [11].

The UMS BoT approved the UMS Strategic Outcomes statement in July 2014. The UMS was identified as being in "… a period demanding transformative change …" and would achieve these outcomes" …through an intensely collaborative approach …" (UMS 2014 Strategic Outcomes, p 1). Collaboration was specific addressed through Strategic

Integration Target 2 that calls for the UMS to "Develop and implement a comprehensive financial management structure for the entire System that enhances transparency, enables appropriate fiscal control, and advances comprehensive intra-system collaboration."(p.1)

Finally, intra-institution cooperation is being fostered through Strategic Integration Target 4 that calls for the UMS to "Develop a model of academic program and portfolio review and integration that leverages academic resources to enhance program quality, expand access, and meets appropriate financial benchmarks, with at least three pilot projects underway in FY15"(p.2)

The UMS established the Academic Portfolio Review and Integration Process (APRIP) process during fall 2014 to bring about academic program integration. The process utilizes two approaches (program integration, portfolio review) to address Strategic Integration Target 4 [12].

Nine discipline-based teams led by faculty members and involving over 100 participants system-wide to develop recommendations for new multi-institutional collaborations that can increase quality, access, and fiscal sustainability are addressing academic program integration.

Academic portfolio review is being addressed by a multi-year process to make program inventory decisions systemically rather than in the silos of individual universities. Members of the Presidents Council and the Chief Academic Officers are to identify academic programs that are less able to meet two or more of three criteria: (1) centrality to institutional mission as differentiated through Strategic Integration Target 1, (2) fiscal sustainability, and (3) meeting the needs of the state.

The calls for increased collaboration and cooperation, especially in light of increasing financial pressure and the concomitant need to accomplish more with less, combined to provide the catalyst for academic program reformation within the UMS.

Key cybersecurity faculty, instructional resources and related academic programs have slowly evolved at four of the UMS universities within the UMS. For example, the University of Maine at Fort Kent was the first post-secondary education institution in Maine to offer an Associate of Science in Information Security and subsequent academic concentration and certificate option. The University of Maine has regularly prepared and fielded a student team at the annual Northeast Collegiate Cyber Defense Competition. The University of Maine at Augusta has excelled in providing cybersecurity instruction, an academic concentration and certificate to the adult non-traditional population. The University of Southern Maine has very successfully garnered grants and industry support and involvement in its establishment of the Maine Cyber Security Cluster (MSCS) [13] that aims to combat and mitigate risk by 1) training cyber security personnel, 2) conducting assessments in lab and at

sites, and 3) providing space, resources, and expertise for cybersecurity research and development. This center also houses as a virtual cybersecurity collaborative learning environment that promotes inter-institutional, innovative, hands-on collaborative learning experiences aimed at preventing and mitigating cyber-attacks in real time [14].

These cybersecurity-related faculties, curricula, instructional laboratories resources, student engagements, research contributions, and community engagement activities have slowly evolved. With respect to the NSA CAE IA/CD program application process, no single UMS university could generate sufficient evidence to achieve recognition. Key faculty members at each of the four UMS universities, upon realizing the synergy that existed, initiated an effort to combine their respective accomplishments and jointly apply for NSA/DHS recognition of the UMS as a shared/distributed CAE IA/CD.

The effort and successful application process received significant support from academic, governmental and industry leadership and in October 2014, the NSA/DHS designated the University of Maine System as a CAE IA/CD through academic year 2019.

The Chancellor of the UMS cited the success of this faculty initiative in his biennial State of Higher Education in Maine presentation to the Joint Session of the 127th Maine Legislature:

> "The University of Maine System benefits from hundreds of able faculty dedicated to their profession and their students, but whose efforts are also constrained by university and bureaucratic silos. Teams of faculty and staff from across Maine are breaking down those barriers and re-imagining their programs, drawing resources from every corner of every university in order to develop student-focused scholarship, with priorities given to academic programs that meet demonstrated community needs.

> Here is an early and resoundingly successful example of where we are going. This past fall the University of Maine System was designated a National Center of Excellence in Cybersecurity Education by the NSA/Dept. of Homeland Security. No individual Maine institution had the resources or expertise to achieve this designation, but by working collaboratively, faculty from UMFK, UMA, UM, and USM created a unified program which earned Maine the nation's first ever multi-university, System designation... It is my honor to recognize [the] Professors whose vision, creativity, and expertise has secured Maine this opportunity, and whose work is an outstanding example of what we can accomplish when we work together."

Getting a Bachelor of Science in Cybersecurity program stood up in the UMS can be considered an example of the "which came first, the chicken or the egg?" There is an urgency to getting the degree program going, but the University of Maine System has no mechanism for offering a system-wide degree. Degrees are offered by the individual universities. The universities have different procedures for approving degree programs. Consequently, the program approval process has proceeded along somewhat different approval lines at each university.

In parallel with the process of establishing the degree program is an effort by the administrations at each of the universities to adopt a Memorandum of Understanding (MOU) defining how the universities will handle some of the inter-university issues. The work on the MOU is being handled by the administrations of the participating universities and is outside the scope of this paper.

Cybersecurity Requirements (36 hours)

CYB 100 Introduction to Computer Science	4 hours
CYB 200 Introduction to Information Security	3 hours
CYB 250 Introduction to Programming	3 hours
CYB 300 Computer Programming	3 hours
CYB 330 Networking	3 hours
CYB 340 Cyber Ethics	3 hours
CYB 350 Databases	4 hours
CYB 360 Network Security	4 hours
CYB 370 Operating Systems Security	3 hours
CYB 390 Cybersecurity Internship (or 2-course alternate)	3 hours
CYB 400 Cyber Defense (Capstone)	3 hours
Cybersecurity Portfolio (see *Techniques for Assessment*)	
	36 hours

Figure 2. Proposed Curriculum

An Academic Governance Board consisting of key faculty and staff from participating universities has driven the process. This group adopted the model curriculum shown in Figure 2 that derives from the curriculum specified in the NSA CAE IA/CD application.

Students are required to complete a Cybersecurity Portfolio in addition to those courses defined within the program. Students construct a portfolio from the projects completed as part of the major course requirements portion of the program. The portfolio is intended to enable assessment of those learning outcomes that are best assessed in an integrative fashion, spanning all of the student's course work and therefore reflects overall academic growth.

4   Recommendations

Given increased pressure upon public post-secondary education institutions by local, regional and national entities to accomplish more with less and continuously improve service to their respective constituencies, the case for increased intra-university collaboration and cooperation is clear. The time to embrace change, consider new approaches, realize synergy through collegial engagement is, or likely soon will be, upon all such institutions.

4.1   Maintain a willingness to listen and a desire to advance the cause through change. Do not become ensnared in callous recalcitrance. Seek out those who are similarly open to change. Explore initiatives that achieve mutually rewarding benefits/outcomes.

4.2   Identify the goals and explore new and/or untried approaches to achieve them. Avoid working in a vacuum or falling back to being a singular source of ideas. Reach out to those with whom you have not previously engaged (students and staff included) to share perspectives and engage in brainstorming approaches. Recall the words of John Donne, "No man is an island, entire of itself." [15]

4.3   Capture the potential of synergies that exist only when two or more collaborate, cooperate, or share and view the "whole is *other* than the sum of the parts" as suggested by Gestalt theory. Such synergistic potential can be substantial, as exemplified in the NSA/DHS recognition of the UMS as a shared/distributed CAE IA/CD.

The establishment of a shared/distributed CAE IA/CD is expected to avail new opportunities to the UMS. One example is the potential to establish new shared/distributed academic degree programs. The establishment of such programs is similarly fostered and supported by the same contextual challenges and opportunities presented.

5   Conclusion

The UMS is the first multi-university entity to achieve NSA/DHS recognition as a *shared/distributed* CAE IA/CD. The challenges and opportunities that most significantly influenced this achievement arose from a geographic, governmental, and administrative context ripe for change.

This context strongly favored vastly increased collaboration and cooperation among the universities within the UMS that formerly evolved their functioning as a loosely coupled federation. As exemplified by the experiences presented, it is possible to better harness the potential synergy resulting from direct engagement in mutually rewarding collaboration and cooperation to achieve significant gains in preparing the future cybersecurity workforce.

6   References

[1]   National IA Education & Training Programs (2015). "CAE Requirements and Resources". Retrieved from https://www.iad.gov/NIETP/CAERequirements.cfm

[2]   National IA Education & Training Programs (2015). "About CAE Program". Retrieved from https://www.iad.gov/NIETP/aboutCAE.cfm

[3]   National IA Education & Training Programs (2015). "Welcome". Retrieved from https://www.iad.gov/iad/index.cfm

[4]   University of Maine System (2015). "Chancellor's Office".
      Retrieved from
      http://www.maine.edu/about-the-system/chancellors-office/

[5]   A. McGettrick (2013). "Toward Curricular Guidelines for
      Cybersecurity: Report of a Workshop on Cybersecurity
      Education and Training". Association of Computing Machinery
      (ACM). Retrieved from
      https://www.acm.org/education/TowardCurricularGuidelinesCy
      bersec.pdf

[6]   L. Hoffman, D. Burley & C. Toregas (2012). "Thinking Across
      Stovepipes: Using a Holistic Development Strategy to Build the
      Cybersecurity Workforce". IEEE Security & Privacy
      Magazine. DOI: 10.1109/MSP.2011.181.

[7]   E. McDaniel (2013). "Securing the Information and
      Communications Technology Global Supply Chain from
      Exploitation: Developing a Strategy for Education, Training,
      and Awareness". Issues in Information Science and Information
      Technology. Retrieved from
      http://iisit.org/Vol10/IISITv10p313-324McDaniel0083.pdf

[8]   D. Rowe, B. Lunt & J. Ekstrom (2011). "The Role of Cyber-
      Security in Information Technology Education", Proceedings of
      the Special Interest Group on Information Technology
      Education (SIGITE), October 2011, pp. 113-121.

[9]   C. Cousins (2015). "LePage's willingness to broaden sales tax
      base surprises some lawmakers". *Bangor Daily News.*
      Retrieved from
      http://bangordailynews.com/2015/01/09/politics/state-
      house/lepages-willingness-to-drastically-broaden-sales-tax-
      base-surprises-some-lawmakers/

[10] University of Maine System (2015). "About Mission Excellence
      at Maine's Public Universities". Retrieved from
      http://thinkmissionexcellence.maine.edu/about-thinkme/

[11] University of Maine System (2012). "Board of Trustees Goals
      and Actions". Retrieved from
      http://thinkmissionexcellence.maine.edu/messages-from-the-
      chancellor-2/goals-and-actions/

[12] University of Maine System (2013). "Academic Portfolio
      Review & Integration Process". Retrieved from
      http://thinkmissionexcellence.maine.edu/priority-
      initiatives/academic-review/

[13] Maine Cyber Security Cluster (2014). "About Us". Retrieved
      from http://www.mcsc.usm.maine.edu/aboutus.php

[14] J. Murphy, E. Sihler, M. Ebben, L. Lovewell, & G. Wilson,
      (2014). "Building a Virtual Cybersecurity Collaborative
      Learning Laboratory (VCCLL)", *Conference Proceedings, SAM
      '14 Conference.* Las Vegas, NV 2014 World Congress in
      Computer Science, 2014. Retrieved from
      http://worldcomp-proceedings.com/proc/p2014/SAM4153.pdf

[15] Donne, John (1623). "Devotions upon Emergent Occasions".
      Retrieved from Project Gutenberg's Devotions Upon Emergent
      Occasions, by John Donne (p. 108). Retrieved from
      http://www.gutenberg.org/files/23772/23772-h/23772-h.htm