Bachelor of Science in Cybersecurity Program Proposal
Executive Summary

Cybersecurity is an evolving discipline that involves the study of strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure (National Initiative for Cybersecurity Careers and Studies). In addition, this major offers a holistic approach to cybersecurity education by affording students the opportunity to take courses not only in computer science and technology but also in the humanities and social sciences (e.g. Crisis Communication, Human Communication Skills, Philosophy of Social Media, and Security). This document proposes a baccalaureate degree in cybersecurity offered by UMS Partnering Institutions as defined by a “Bachelor of Science in Cybersecurity Online Consortium - Memorandum of Understanding” (MOU). It proposes a 4-year program closely coordinated among the Partnering Institutions that is based on an existing curriculum. The curriculum has recently achieved National Security Agency/Department of Homeland Security (NSA/DHS) recognition as the core component of a UMS distributed Center of Academic Excellence in Information Assurance/Cyber Defense (CAEIA/CD).

The goals of the degree program are to prepare students to fill a gap in Maine’s workforce and provide a smooth articulated path from Maine’s community college system to an accredited Bachelor’s degree from any of the Partnering Institutions. This is a practice-oriented curriculum with opportunities for internships and significant Capstone projects. The program curriculum has been designed to meet the stringent academic standards of the NSA/DHS jointly sponsored CAEIA/CD program. This NSA/DHS recognition program serves as the de facto accreditation standard for Cybersecurity programs.

BS Cybersecurity graduates will meet an employment need in Maine’s IT workforce, significantly improving the statewide prospect for excellence in the computer-based delivery of information security services. Local industry and state government are asking for this program as demonstrated through letters of support for the NSA/DHS CAEIA/CD (ref Appendix).

All program topics have been and continue to be taught by existing faculty among the Partnering Institutions. The financial analysis is strongly positive given that no new resources are required; to the contrary, newfound synergy among the Partnering Institutions and optimized sharing of existing resources are expected to yield savings while extending the effective reach and market potential for this much needed program.
# Bachelor of Science in Cybersecurity Program Proposal

Last Revised April 3, 2015

## Table of Contents

I. Institution and Program Title ................................................................. 5

II. Program Objectives ............................................................................... 6
   A. Narrative description of program rationale ............................................ 6
   B. General program goals (limit to 3-5 major items maximum) .................. 7
   C. Specific student outcomes or behavioral objectives (limit to 5-8, written for public accountability) ................................................................. 8
   D. Accountability .................................................................................. 9

III. Evidence of Program Need .................................................................... 10
   A. For 2-year programs, indicate potential employers who have requested the program and their specific employment projections (support data to be attached) .................. 16
   B. Detailed survey of similar programs that are offered within the University System, other higher education institutions or other agencies within the State ............................................. 16
   C. Enrollment projections for five years .................................................. 18

IV. Program Content .................................................................................. 18
   A. Outline of required and/or elective courses (not syllabi); ....................... 18
   B. Development of new courses and/or what they may displace ................ 23
   C. Type of research activity, if any, in program design ............................... 24
   D. Nature of independent study, clinical experience, and/or field practicums employed in curriculum design .............................................................. 24
   E. Impact of program on existing programs on the campus ....................... 24

V. Program Resources ................................................................................ 25
   A. Personnel ......................................................................................... 25
   B. Current library acquisitions available for new program ......................... 27
   C. New equipment necessary for new program and plan for its acquisition and implementation .......................................................... 27
   D. Additional space requirements, if any, including renovations ................. 27
   E. Extent of cooperation with other programs, both on the initiating campus and other campuses ........................................................................... 27

VI. Total Financial Consideration ................................................................ 28
   A. Estimate of anticipated cost and anticipated income of the program for five years ................................................................. 28
   B. Detailed information on first-year costs, including: ................................ 29

Last Revised April 3, 2015
1. New personnel requirements (including employee benefits): ............................................. 29
2. First-year revenue and identity of source........................................................................ 29
3. How operational costs are to be absorbed into current campus operating budget over a 5-year period ......................................................................................................................... 29
4. What additional funding is required to support the program (identity of source) ........ 29
5. Lifetime of outside or independent funding and plan for how and when – becomes part of E&G budget ................................................................................................................................. 29

VII. Program Evaluation ........................................................................................................... 30

A. A post audit of an approved new program must be made after five years................. 30

APPENDICES ........................................................................................................................... 34

References ............................................................................................................................... 35

B.S. in Cybersecurity Online Consortium – MOU ................................................................. 36

Sample of Support Letters .................................................................................................... 38

Faculty Curriculum Vitae ....................................................................................................... 50

External Reviewers’ Reports .................................................................................................. 91

Preliminary Findings of USM MBA Students’ Market Research ........................................ 101

Financial Model ....................................................................................................................... 107
I. Institution and Program Title

**Partnering Institutions:** (per MOU - ref Appendix) (in alpha order)
- University of Maine
- University of Maine at Augusta
- University of Maine at Farmington
- University of Maine at Fort Kent
- University of Maine at Machias
- University of Maine at Presque Isle
- University of Southern Maine

**Degree:** Bachelor of Science (B.S.)
**Area:** Cybersecurity
**Date of Implementation:** Fall 2015
**Expected Termination Date:** Ongoing
**Format:** Online (hybrid)
**CIP Code(s):** 11.1003

**Persons responsible for planning:**

- **Name:** Dr. Raymond Albert, *Project Leader*,
  **Address:** UMFK, 23 University Dr, Fort Kent, ME 04739
  **Telephone:** 207 834-7696
  **Email:** ralbert@maine.edu

- **Name:** Dr. Christopher Bennett
  **Address:** UMF
  **Telephone:** 207 778-7114
  **Email:** chris.bennett@maine.edu

- **Name:** Dr. Henry Felch
  **Address:** UMA
  **Telephone:** 207 621-3371
  **Email:** henry.felch@maine.edu

- **Name:** Diana Kokoska
  **Address:** UMA
  **Telephone:** 207 262-7864
  **Email:** dkokoska@maine.edu

- **Name:** Dr. George Markowsky
  **Address:** UM
II. Program Objectives

A. Narrative description of program rationale

The Partnering Institutions are proposing a Bachelor of Science in Cybersecurity degree as a new system-wide shared signature program. Our primary goal is to develop a flexible interdisciplinary degree that (1) serves students wishing to earn a degree within 120 credit hours; (2) prepares them for career opportunities or advanced education in the Cybersecurity field; and (3) incorporates a multidisciplinary perspective through a combination of computer science, communications, and ethics courses.

We propose this degree program as one means to address the need for higher education opportunities in this critical need area and provide students the opportunity to seamlessly transition from existing associate degree programs. We therefore anticipate this new degree program will provide a means to meet the needs of future students, improve enrollment across multiple programs and contribute to the Partnering Institutions’ respective missions.

The key aim of the degree program is to address the severe shortage of skilled practitioners in the cybersecurity field and address Maine workforce needs. It will prepare students to better understand, prevent, detect, react, and recover from threats to cybersecurity and simultaneously prepare them for optional professional certification (e.g., ISC² CISSP).

A secondary aim of the degree program is to raise awareness and interest of students in the following closely-related programs of study at the respective institutions of the University of Maine System:

- Master of Science in Computer Science, UM
- Doctor of Philosophy in Computer Science, UM
- Master of Science in Computer Engineering, UM
- Doctor of Philosophy in Computer Engineering, UM
- Post Baccalaureate in Computer Information Systems, UMA
B. General program goals (limit to 3-5 major items maximum)

Program Description/Goals

The Bachelor of Science in Cybersecurity is designed to prepare students to obtain employment in the evolving cybersecurity field or as a course of study leading to graduate studies in cybersecurity.

Vision Statement

The Bachelor of Science in Cybersecurity program will be the preferred interdisciplinary and collaborative leader in Cybersecurity and Information Assurance (IA) education in the state of Maine. We will be recognized throughout the state and nation as a source of knowledge, expertise, and innovation in the fields of Cybersecurity and IA. We will be recognized also for providing ongoing academic leadership in education, research, and practice that empowers our students to be the IS/IT professionals of tomorrow who are capable of meeting this nation's Cybersecurity needs.

Mission Statement

The NSA/DHS recognized UMS distributed Center of Academic Excellence in Information Assurance/Cyber Defense and the Bachelor of Science in Cybersecurity program is an interdisciplinary collaborative that dedicates itself to promoting the study and advancement of Cybersecurity and IA. The Bachelor of Science in Cybersecurity program prepares professionals capable of leading technological changes in industry both locally and nationally, with an emphasis on the protection of technological infrastructures for the preservation of Cybersecurity and IA.

It does this by providing a supportive and instructional learning and research environment in which students meet the challenges of developing and mastering in-depth knowledge, understanding, and skill-sets in the varied domains within Cybersecurity and IA, with hands-on applications in analysis, prevention, deterrence and countermeasures of information security and integrity in a global arena. Students who pursue this program of study will find that hands-on application will enable them to design, implement, and administer the security of information systems by embracing the concepts studied and applying those concepts in laboratory settings.
To achieve this mission, the program faculty and administration:

- Foster and fine-tune the curriculum and student selection process to optimize our role of being a bridge between technology, management, and society,
- Deliver the curriculum through the intelligent use of synchronous, asynchronous learning instructional environments for both full-time and part-time students,
- Promote appropriate student and professional responsibility through a multidisciplinary studies approach,
- Promote instructional excellence that inspires our students to become successful Cybersecurity/IA practitioners,
- Coordinate availability of Cybersecurity and IA coursework to assist Maine and the nation meet their demand for Cybersecurity and IA professionals,
- Develop partnerships and alliances with external corporate and industry organizations for pursuing joint educational and research opportunities in IA;
- Pursue research and grant opportunities in all areas related to Cybersecurity and IA,
- Provide outreach opportunities to K-12 educational levels as well as other interested parties and organizations, and
- Promote Cybersecurity collaboration among colleges, government and industry.

C. Specific student outcomes or behavioral objectives (limit to 5-8, written for public accountability)

Program Description/Goals

The Bachelor of Science in Cybersecurity Program is designed to prepare students to obtain employment in the cybersecurity field or as a course of study leading to graduate studies in cybersecurity.
Student Learning Outcomes

Cybersecurity program graduates will be able to:

1. Apply knowledge of computing and information technologies and use software development and security analysis tools to produce effective designs and solutions for specific cybersecurity problems within a variety of computing platforms and employing an approved secure systems development process model;
2. Identify, analyze, and synthesize scholarly and professional literature relating to the fields of cybersecurity, information security, or information assurance, to help solve specific problems and to stay abreast of the rapidly changing security context;
3. Participate as an active and effective member of a project team engaged in achieving specific computer-based results or solutions;
4. Communicate, both orally and in writing, and negotiate with colleagues and other stakeholders including employees, managers, and executives. Negotiation and communication skills should also extend to all relevant external persons and organizations;
5. Demonstrate sensitivity to and sound judgment on ethical issues as they arise in information security and cyber defense and will adhere to accepted norms of professional responsibility;
6. Integrate knowledge from other disciplines, such as economics, management science, psychology and human factors, with their technical expertise to arrive at practical solutions that work successfully in real organizations; and
7. Use appropriate tools to prevent, detect, react, and recover from attacks.

D. Accountability

This program is unique in Maine, with a focus on optimized use and existing resources distributed across the UMS and the collaborative-based synergy that exists among the Partnering Institutions faculty. It will incorporate existing faculty, courses, and resources to extend a new degree opportunity to students at each of the Partnering Institutions. The program will be reviewed in accordance with all applicable UMS policies, and external accreditation and recognition standards/criteria.

Accountability to stake-holders will be maintained through their continuing involvement as advisory board members. The curriculum, student learning outcomes, and other key elements of the program will evolve with economic and workforce needs, and evolving academic/industry standards.
III. Evidence of Program Need

Consider the following quote that serves to evidence the existing need.

“Security continues to be a primary concern of computer professionals today, and with good reason. Consider the evidence: the number of malware attacks against online banking is increasing annually by 60,000, and 85 percent of banks reported that they have sustained losses based on these attacks. Over $41 billion have been lost by victims to the Nigerian General scam, which is the number one type of Internet fraud and is growing at a rate of 5 percent. Over 20 million new specimens of malware, including new malware as well as variants of existing families, were created in one eight-month period, and the average number of new threats created and distributed each day has increased from 55,000 to 63,000. Due to increased power of desktop computers to crack passwords, researchers now claim that any password of seven or fewer characters is “hopelessly inadequate”. And a computer connected to the Internet is probed by an attacker on average once every 39 seconds.

As these types of attacks continue to escalate, the need for trained security personnel also increases. Unlike some information technology (IT) functions, security is neither being offshored nor outsourced. Because security is such a critical element in an organization, security functions generally remain within the organization. In addition, security positions do not involve “on-the-job training” where untrained employees can learn as they go; the risk is simply too great.” (2012, Ciampa)
“Cyber attacks, or breaches of information security, and the severity of these attacks in government, military and commercial sectors are increasing in frequency as the integration of computers into more aspects of modern life continues (McAfee, 2011). The year 2013 pushed cybersecurity further into the spotlight as it featured the President’s executive order, an orchestrated cyber-attack on South Korea, the Mandiant APT1 report, the NY Times and Wall Street Journal Breaches, Edward Snowden, and Target, to name a few. These and other events have escalated the status of cybersecurity issues making them top priorities for national/state governments, law enforcement, and corporate boards of directors (Oltsik, 2014b). Figure 1 is a graphical representation of the scale and volume of cybersecurity exploits that are occurring on a daily basis.

![Figure 1: World-Wide Breaches](http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches/)

A recent joint study by the nonprofit Center for Strategic and International Studies (2013) and the computer-security firm McAfee posits a $100 billion annual loss to the U.S. economy and as many as 508,000 U.S. jobs lost as a result of malicious cyber activity (CSIS, 2013). Global losses, it finds, are between $100 billion and $500 billion each year. This new estimate reflects a major revision of McAfee’s own previous estimate of $1 trillion (Maass & Rajagopalan, 2012; Vamosi, 2012), which has been cited widely, including by U.S. Government officials. These losses result from cyber-attacks in six categories: the loss of intellectual property, cybercrime, and loss of business information, service disruptions, and the cost of securing networks, and reputational damage to a hacked company.

Market Research Media (MRM) reports that with a cumulative market valued at $65.5 billion between 2013 and 2018, the U.S. Federal Cybersecurity market will grow steadily at about 6.2% over the next six years (MRM, 2013). Companies will spend an estimated $75 billion, or an average of 5 percent of their IT budget on security. Drivers for security spending include targeted malicious software attacks, cybercrime, regulation, remote access and new delivery models for services. Companies ranked intrusion detection and
prevention as the top security priority, followed by patch management, data loss prevention, identity management and antivirus.

President Obama efforts to secure cyberspace. “In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults both in the private sector and the public sector. Now, our first order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place...But even as we get better, the hackers are going to get better, too. Some of them are going to be state actors; some of them are going to be non-state actors. All of them are going to be sophisticated and many of them can do some damage.

This is part of the reason why it’s going to be so important for Congress to work with us and get an actual bill passed that allows for the kind of information-sharing we need. Because if we don’t put in place the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movies, this is going to be affecting our entire economy in ways that are extraordinarily significant.” (President Obama, December 19, 2014)

Shortage in trained cybersecurity workers. With billions of dollars in global losses due to cybersecurity exploits, the need for trained experts is growing at an astonishing rate. The U.S. Bureau of Labor Statistics is predicting 22% growth in employment in cybersecurity by 2020. The federal government is actively recruiting to fill 10,000 cybersecurity professional positions, of which approximately 5,000 of these positions are at the U.S. Cyber Command. Aggressive growth in training will be critical to the catch-up effort. Such efforts include IBM's Cybersecurity Innovation Program and its new university partnerships around the world, the National Initiative for Cybersecurity Education (NICE), and the strong academic programs at the University of Maryland, the University of Texas at Dallas, the University of Southern California, Purdue University, Northeastern University, and the University of Michigan.

In Maine, there is a need to improve workforce education and development opportunities for the IT community, specifically centered on cybersecurity. IT is one of Maine’s high-growth occupations but current conventional training and educational models are not producing enough qualified graduates to meet the demand from IT employers for skilled candidates. This is true throughout Maine but particularly in greater-Portland. Based on information gathered from the University of Maine System (UMS) - Business Computer Science and Information Technology Partnership, as much as 30% of the state’s IT workforce is expected to be lost to retirement in the next five years. The overwhelming response from the Partnership participants was that if their
companies could not find IT-skilled technical workers in Maine, and preferably from the Portland area, they would be forced to seek skilled IT professionals outside of Maine. Based on the aggregate requirements of the employer partners, there is a need to fill over 400 IT positions in the six IT occupations in the next four years (Computer Programmers, Computer Software Engineers, Applications, Computer Software Engineers, Systems Software, Computer Specialists, Computer Support Specialists, and Network and Computer Systems Administrators, including Computer Security Specialists). These six occupations are in the top ten fastest growing IT occupations in Maine. Maine Employment Outlook to 2018 published by Maine Department of Labor, projects a demand of approximately 240 openings per year for the six occupations due to both growth and replacement.

The ongoing shortage of qualified cybersecurity IT professionals is creating a set of problems that goes well beyond the immediate security of data and systems. The shortage is also inhibiting the effective adoption of key technologies in the enterprise and the public sector, including mobile, cloud and social applications, among others. And that will, in turn, inhibit enterprise growth and economic expansion (Shaw, 2013). Cyber criminals are well organized and highly skilled yet the U.S.’s cybersecurity workforce is undermanned and under skilled.

**National Cybersecurity Workforce Framework.** An essential step to ensuring that our nation can educate, recruit, train, develop and retain a highly qualified cybersecurity workforce is a common understanding of and lexicon for cybersecurity work. To this end, NICE recently established the National Cybersecurity Workforce Framework, which is for the public, private, and academic sectors using a common taxonomy and lexicon that describe all cybersecurity work and workers irrespective of where or for whom the work is performed. The Framework consists of thirty-one specialty areas organized into seven categories (Figure 2) that serve as an overarching structure for the Framework, grouping related specialty areas together and including each specialty area’s requirements for typical tasks and knowledge, skills, and abilities.
The need for skilled practitioners in the cybersecurity field is so great that the federal government has reported continuation of a three-year backlog in unfilled positions. Funding opportunities made available under the auspices of the National Science Foundation have been created to provide full funded scholarships to students who agree to complete graduate degrees in the field and agree to serve as civil servants for a like number of years.

The Department of Defense (DoD) issued in 2008 a directive (Directive 8570) that provides guidance and procedures for the training, certification, and management of all government employees who conduct Information Assurance functions in assigned duty positions. These individuals are required to carry an approved certification for their particular job classification. It affects any full- or part-time military service member, contractor, or local nationals with privileged access to a DoD information system performing information assurance (IA) functions -- regardless of job or occupational series. The directive requires:

- 100% of the IA professionals in DoD and DoD contractors must be certified within the next 3 years,
- 40% must be certified by the end of 2008,
- All IA jobs will be categorized as 'Technical' or 'Management' Level I, II, or III, and to be qualified for those jobs, you must be certified.

Recent reports indicate that only 30% of the approximately 90,000 affected employees have so far met the mandated requirements.

Many other federal initiatives specifically identify the need to increase awareness and attention to cybersecurity through increased funding opportunities. Consider the following recent examples:

- Cybersecurity Act of 2009 (S. 773 under consideration and co-sponsored by Senator Olympia Snowe)
  - “A bill to ensure the continued free flow of commerce within the United States and with its global trading partners through secure cyber communications ... to provide for the development of a cadre of information technology specialists to improve and maintain effective cybersecurity defenses against disruption, and for other purposes.” (April, 2009)

  - Near term action plan calls for, among other things, “the United States needs a technologically advanced workforce to remain competitive in
the 21st Century economy... The United States should initiate a K-12 cybersecurity education program for digital safety, ethics, and security; expand university curricula; and set the conditions to create a competent workforce for the digital age. … the Nation should:

- Promote cybersecurity risk awareness for all citizens;
- Build an education system that will enhance understanding of cybersecurity and allow the United States to retain and expand upon its scientific, engineering, and market leadership in information technology;
- Expand and train the workforce to protect the Nation’s competitive advantage; and
- Help organizations and individuals make smart choices as they manage risk." (DHS, June, 2009, p. 13)

UMFK graduates have recently filled Maine-based positions advertised by the Maine State Police (computer forensics investigations), banking institutions (e.g., NorState Federal Credit Union, Kennebec Savings Bank, Camden National Bank), as well as other organizations and businesses. These graduates serve in computer and network security services with knowledge of computer forensics and penetration testing (important cybersecurity functions).

The popular INDEED job search website regularly posts positions that require computer and/or cybersecurity preparation and/or experience. Recent examples in Maine include:

- **Information Security Officer** - General Dynamics Bath Iron Works - Bath, ME
- **IT Security Specialist** - General Dynamics Bath Iron Works - Bath, ME
- **Cybersecurity Analyst II** - T2E Solutions, Inc - Springfield, ME
- **Information Security Specialist** - Goldbelt, Inc. - Kittery, ME
- **Security Administrator I** - WEX Inc. – South Portland, ME
- **Cyber Security Professional** – NTT Data, Inc. – Freeport, ME
- **Head of Application Security** – TD Bank – Falmouth, ME
- **Security Architect** – Deutsche Bank – Harborside, ME
According to the *Maine IT Skills Census Report* (Nov. 2009, p. 14), “The workforce has indicated their desire for additional educational opportunities… [The survey] indicates the existing workforce working towards certification in: … Security …” By providing more educational and certification opportunities within the state the reliance upon out-of-state providers will be greatly reduced.

Professor Glenn Wilson (USM) has enlisted the assistance of a group of USM MBA students to conduct an informal market research project during the Spring 2015 term. Their preliminary findings (see Appendix) are promising and the students are now entering the most exciting part of their research - beginning interviews with various companies and other entities in Maine. They intend to share with all interested UMS parties their final report, including key findings. These market research findings will certainly provide an even clearer understanding of program need and, in turn, contribute to further program improvements.

A. For 2-year programs, indicate potential employers who have requested the program and their specific employment projections (support data to be attached)

N/A

B. Detailed survey of similar programs that are offered within the University System, other higher education institutions or other agencies within the State

The National Center of Education Statistics (NCAS) has established a Classification of Instructional Programs (CIP) code in recognition of this relatively new field of study. The CIP code is 11.1003 and it represents Computer and Information Systems Security/Information Assurance.

Thomas College has recently made available a Bachelor of Science in Security and Cyber-Defense. The program has yet to be recognized as a NSA/DHS CAEIA/CD.

There are a number of IA/CD-related degree programs within the UMS as depicted in Table 1.

**Table 1: IA/CD-Related Degree Programs**

<table>
<thead>
<tr>
<th>Institution</th>
<th>Degree Programs</th>
</tr>
</thead>
<tbody>
<tr>
<td>UM</td>
<td>Bachelor of Science in Computer Science, Master of Science in Computer Science, and PhD in Computer Science</td>
</tr>
</tbody>
</table>
There also exists a focus on cybersecurity education at the community college level. With funding from a 2013 Department of Labor Trade Adjustment Assistance Community College and Career Training (TAACCCT) grant, the YCCC is developing a Cybersecurity Certification program. In addition to adding value to YCCC’s Certificate Program, the proposed virtual Cybersecurity Laboratory will positively impact other cybersecurity education initiatives in Maine. For example, USM just completed the development of a new Bachelor’s of Science in Information Technology degree, which requires three cybersecurity courses in its curriculum. Moreover, YCCC, Southern Maine Community College, and Central Maine Community College have signed off on a Memorandum of Understanding for a 2+2 or “completer” program for the BSIT. YCCC is a founding and key player in the BSIT as well as this project.

Examples of other public and private non-profit universities that offer related programs include the following (Source: [http://nces.ed.gov/collegenavigator](http://nces.ed.gov/collegenavigator))

- Norwich University (Bachelor of Science - Computer Security & Information Assurance)
- Champlain College (Bachelor of Science in Computer Networking & Cybersecurity)
- Rochester Institute of Technology (Bachelor of Science in Computing Security)
- Towson University (Bachelor of Science in Computer Science with a Computer Security track and a Master of Science in Computer Science with a Computer Security track)
- Drexel University (Bachelor of Science in Computing & Security Technology)
• Kennesaw State University (Bachelor of Business Administration - Information Security and Assurance)

• High Point University (Bachelor of Science in Cybersecurity and Privacy)

C. Enrollment projections for five years

<table>
<thead>
<tr>
<th>Year</th>
<th>Projected Total Enrollment*</th>
</tr>
</thead>
<tbody>
<tr>
<td>AY 15/16</td>
<td>15</td>
</tr>
<tr>
<td>AY 16/17</td>
<td>30</td>
</tr>
<tr>
<td>AY 17/18</td>
<td>45</td>
</tr>
<tr>
<td>AY 18/19</td>
<td>60</td>
</tr>
<tr>
<td>AY 19/20</td>
<td>60</td>
</tr>
</tbody>
</table>

* Across all Partnering Institutions

These enrollment projections are intentionally conservative that they may reflect the least favorable financial impact scenario for the program. Actual enrollments are expected to be greater, depending on the degree of support provided to a strong roll-out of the program and establishment of a strong program image in the eyes of the students, employers, and Maine citizenry.

The financial model (ref Appendix) takes builds upon these enrollment projections and it also takes into account other factors affecting year-to-year enrollments such as historical retention trends in related degree programs (e.g., CS).

IV. Program Content

A. Outline of required and/or elective courses (not syllabi);

Special note: The following reflects a “prototype curriculum”. Precise specification of suitable course numbers/titles amenable to a “system-oriented” degree is under development pending formal program approval. The final curriculum will be established upon program approval, prior to student matriculation, and its mapping to NSA/DHS CAEIA/CD curriculum Knowledge Units will be maintained.
Bachelor of Science in Cybersecurity

The security of information assets is one of the most pressing concerns facing our information age society. The Cybersecurity degree prepares students to better understand, prevent, mitigate and respond to threats to cybersecurity. Students are introduced to basic Cybersecurity concepts, current issues and approaches to Cybersecurity and they are prepared for optional professional certification (e.g., ISC² CISSP). Consistency with national, regional, state efforts relating to the evolution of Cybersecurity as a field will remain a top concern. The following efforts continue to guide the definition and use of the term “Cybersecurity” as it evolves from “computer security”, “network security”, “information security”, and “information assurance”:

The National Cybersecurity Workforce Framework, developed by the National Initiative for Cybersecurity Education (NICE) under the auspices of the National Institute of Standards and Technology (NIST), establishes the common taxonomy and lexicon that is to be used to describe all cybersecurity work and workers irrespective of where or for whom the work is performed. The Framework is intended to be applied in the public, private, and academic sectors.

DoD Instruction 8500.01 (March 14, 2014) calls for the adoption of the term “Cybersecurity”, as it is defined in National Security Presidential Directive-54/Homeland Security Presidential Directive-23, to be used throughout DoD instead of the term “information assurance (IA).” The same instruction defines Cybersecurity as “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.”

Most critically, adherence to evolving standards for accreditation/recognition (e.g., NSA/DHS CAEIA/CD) will be maintained.
General Education Requirements
(as defined by each Partnering Institution)

For example – USM requires the following:

1. Entry year experience
2. College Writing
3. Quantitative Reasoning
4. Creative Expression
5. Cultural Interpretation
6. Socio-cultural Analysis
7. Science Exploration
8. Diversity
9. International
10. Ethical Inquiry, Social Responsibility, and Citizenship
11. Capstone in the major

For example – UMFK requires the following:

1. Intellectual and Practical Skills (19-20 hours):
   a. Communication (9 hours)
      i. Written
      ii. Oral
   b. Quantitative Reasoning (6 hours)
   c. Information Fluency (4 hours)
2. General Knowledge (19-22 hours)
   a. Arts & Humanities (12-15 credits)
      i. Visual & Performing Arts (3 hours)
      ii. Literature (3 hours)
      iii. History (3 hours)
      iv. Foreign Language (3-6 hours)
   b. Natural Sciences (4 hours)
   c. Behavioral-Social Sciences (3 hours)
3. Personal and Social Responsibility

Essential Prerequisites for Student Matriculation into Program

COS 103 Introduction to Information Technology (or comparable)
MAT 128 College Algebra or MAT 165 Pre-Calculus (or comparable)
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  

Students may, based on availability, pursue  
CYB 275 Policy, Law, Compliance, Ethics – I 3 hours  
CYB 375 Policy, Law, Compliance, Ethics – II 3 hours  
CYB "IA Focus Area" electives [6 hours]  

Electives 30-34 hours  
120 hours

Techniques for Assessment

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.
### Suggested Course Sequencing (Sample Plan)

#### Fall Semester Freshman Year
- General Education course
- General Education course
- General Education course
- General elective
- CYB 200 Introduction to Information Security

<table>
<thead>
<tr>
<th>Course</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General elective</td>
<td>3</td>
</tr>
<tr>
<td>CYB 200 Introduction to Information Security</td>
<td>3</td>
</tr>
</tbody>
</table>

15 hours

#### Spring Semester Freshman Year
- General Education course
- General Education course
- General elective
- General elective
- CYB 100 Introduction to Computer Science

<table>
<thead>
<tr>
<th>Course</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General elective</td>
<td>3</td>
</tr>
<tr>
<td>General elective</td>
<td>3</td>
</tr>
<tr>
<td>CYB 100 Introduction to Computer Science</td>
<td>4</td>
</tr>
</tbody>
</table>

16 hours

#### Fall Semester Sophomore Year
- General Education course
- General Education course
- General elective
- CYB 250 Introduction to Programming
- CYB 330 Networking

<table>
<thead>
<tr>
<th>Course</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General elective</td>
<td>3</td>
</tr>
<tr>
<td>CYB 250 Introduction to Programming</td>
<td>3</td>
</tr>
<tr>
<td>CYB 330 Networking</td>
<td>3</td>
</tr>
</tbody>
</table>

15 hours

#### Spring Semester Sophomore Year
- General Education course
- General Education course
- General elective
- CYB elective
- CYB 300 Computer Programming

<table>
<thead>
<tr>
<th>Course</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General Education course</td>
<td>3</td>
</tr>
<tr>
<td>General elective</td>
<td>3</td>
</tr>
<tr>
<td>CYB elective</td>
<td>3</td>
</tr>
<tr>
<td>CYB 300 Computer Programming</td>
<td>3</td>
</tr>
</tbody>
</table>

15 hours
Fall Semester Junior Year
General Education course 3 hours
General Education course 3 hours
General elective 3 hours
CYB 350 Databases 4 hours
CYB 360 Network Security 3 hours

Spring Semester Junior Year
General Education course 3 hours
General Education course 3 hours
General Education elective 3 hours
CYB elective 3 hours
CYB 340 Cyber Ethics 3 hours

15 hours

Fall Semester Senior Year
General elective 3 hours
General elective 3 hours
General elective 3 hours
CYB elective 3 hours
CYB 370 Operating Systems Security 3 hours

15 hours

Spring Semester Senior Year
General elective 3 hours
General elective 3 hours
CYB elective 3 hours
CYB 390 Computer Management Internship (or two course alternate) 3 hours
CYB 400 Cyber Defense (Capstone) 3 hours

15 hours

B. Development of new courses and/or what they may displace

No new courses will be needed to implement this program. It is expected that the curriculum will evolve with new/revised courses to remain in concert with
pertinent accreditation/recognition criteria. Additional funding may be necessary to develop any new course required in the future.

C. Type of research activity, if any, in program design

Students will be expected to conduct course-based undergraduate research activities. For example, students will be required to research and prepare reports on topics related to their Capstone Projects.

Students will also be provided the opportunity to participate in Cybersecurity research activities being conducted at the Maine Cybersecurity Cluster (MCSC) at USM. For example, students from UMFK, USM, and York Community College will be engaged in a CyberCorp simulation activity during March 2015. The National Science Foundation (NSF) funded project is focused on exploring the effects of student involvement in a Cybersecurity “Collaboratory” among other things. USM students have established their own Cyber Security Organization.

A Homeland Security Lab in 221 East Annex at UM also exists. Speakers have been invited throughout the Fall 2014 semester. Also, UM has established a Cybersecurity Club & NECCDC Team. They have a lab in East Annex, and George Markowsky serves as their coach.

D. Nature of independent study, clinical experience, and/or field practicums employed in curriculum design

Students will be required to complete experiential/service learning activities as part of their coursework. Students will also have the opportunity to complete an internship at an approved organization. Student internships will be managed by program faculty in accord with existing policies. Internship experience may require proof of insurance, security clearance and the like as students will be engaged in activities that are often of a sensitive/confidential nature.

E. Impact of program on existing programs on the campus

The program is expected to entice and serve a much larger student market than is currently being served by related programs at disparate UMS institutions. Student preference for local (face-to-face) completion of a majority of their coursework remains high but continues to evolve as students also wish to avail themselves of unique resources available within the UMS.
More students will likely enroll in existing and planned Associate-level degree programs both within the UMS (e.g., Associate of Science in Information Security at UMFK) and within the Maine Community College System knowing that they may seamlessly transition into this Bachelor-level degree program.

The program is also envisioned to serve as a feeder for graduate degree programs that will eventually be developed at either/both UM and USM.

Implementation of the proposed program will lead to increased course enrollments and more efficient utilization of limited faculty resources than currently exists. The Academic Governance Council (ref. CAEIA/Cyber Defense) and Leadership Committee (ref. MOU) will ensure continued oversight of the curriculum and coordination of faculty assignments and other resources to ensure program quality and continuous improvement.

V. Program Resources

A. Personnel

1. Vita of faculty who will assume major role for program to be included in appendix

   Refer to Appendix.

2. Specific effect on existing programs of faculty assignments to new program. List necessary faculty adjustments.

   No new personnel are required to support the offering of this program. Faculty personnel currently employed by the Partnering Institutions are uniquely qualified to offer courses in Cybersecurity and related areas vis-à-vis their graduate school preparation and professional experience. It is envisioned that staff support will continue to be provided by the UMS, the Partnering Institutions and external agencies in proportion to efforts to further optimize utilization of resources through collaboration and in light of program growth.

   Existing programs of study for which faculty may be involved will continue to operate unimpeded. Workload assignments will be negotiated in accord with existing policies and agreements (e.g., AFUM). An Academic Governance Council, consisting of the following
individuals will prepare recommendations for course load assignment per MOU stipulations.

Full-time and part-time program faculty include:

**Raymond Albert, Ph.D.**
Professor of Computer Science

**David Briggs, Ph.D.**
Professor of Computer Science

**Maureen Ebben, Ph.D.**
Lecturer in Communication

**Henry Felch, D.C.S.**
Assistant Professor of Computer Information Systems

**Charles Largay**
Adjunct Professor

**George Markowsky, Ph.D.**
Professor of Computer Science

**Linda Markowsky, Ph.D.**
Assistant Research Professor

**Julien Murphy, Ph.D.**
Professor of Philosophy

**Mark Rosenbaum, Ph.D.**
Adjunct Professor

**Edward Sihler**
Adjunct Professor

**Glenn Wilson, Ph.D.**
Associate Research Professor
B. Current library acquisitions available for new program

No new library resources are required to support the offering of this program. Library resources currently available at the Participating Institutions and within the UMS are sufficient to fully support this program.

C. New equipment necessary for new program and plan for its acquisition and implementation

No new equipment is required to support the offering of this program. Equipment currently available at the Partnering Institutions is sufficient to fully support this program. It is envisioned that equipment support will continue to be provided by the UMS, the Partnering Institutions and external agencies in proportion to efforts to further optimize utilization of resources through collaboration.

As the program grows, it is expected that new equipment/funds will be required to ensure adequacy of virtual laboratory resources both within the UMS and commercially (e.g., NETLAB, Amazon EC2) respectively.

D. Additional space requirements, if any, including renovations

No new facilities are required to support the offering of this program. It is envisioned that additional space will be provided by the UMS, the Partnering Institutions and external agencies in proportion to efforts to further optimize utilization of resources through collaboration and to enrollment increases beyond that which is expected.

E. Extent of cooperation with other programs, both on the initiating campus and other campuses

This feasibility of this program rests in the informal collaboration forged among the Partnering Institutions. A MOU (ref Appendix) has evolved to formalize the collaborative relationships. The recently announced NSA/DHS recognition of the distributed UMS Center of Academic Excellence in Information Assurance/Cyber Defense stands as a covenant to continued progress and evolution of this and other programs envisioned for the future.
Every effort will be made to extend the reach of this program to the entire citizenry of Maine through the use of distance, local, and blended course delivery modalities. Similarly, UMS universities not yet signed on as a Partnering Institution will be encouraged to join.

Students who meet all degree requirements will graduate and receive a diploma from their respective Partnering Institution as stipulated in the MOU.

VI. Total Financial Consideration

In accordance with the BS in Cybersecurity MOU, program tuition and fees shall be set by approval of the University of Maine System. Each home institution will bill and collect tuition and fees from its enrolled students, as well as award financial aid and process billing and enrollment certification for Veterans Affairs educational benefits. As needed, policies regarding fiscal matters will be developed by the Leadership Committee as specified in the MOU.

Consortium members will agree to a program price and to a revenue share plan for each program offered through this arrangement. Details of the program price(s) will be included as addenda to the MOU as agreed upon by member institutions.

No additional costs are required to support first-year and subsequent year operations as courses are a part of existing curricula and are regularly offered by existing faculty resources.

First year and subsequent revenue are a function of the number of students enrolled in the program.

Increased optimization in the use of distributed resources is expected to yield support for continued program improvement.

A. Estimate of anticipated cost and anticipated income of the program for five years.

A financial model, including anticipated income, expenses and associated financial factors, based on defined assumptions, has been prepared for the first five years of the program (ref Appendix)
B. Detailed information on first-year costs, including:

1. New personnel requirements (including employee benefits):

   N/A

2. First-year revenue and identity of source

   A financial model, including anticipated income, expenses and associated financial factors, based on defined assumptions, has been prepared for the first five years of the program (ref Appendix)

3. How operational costs are to be absorbed into current campus operating budget over a 5-year period

   A financial model, including anticipated income, expenses and associated financial factors, based on defined assumptions, has been prepared for the first five years of the program (ref Appendix)

4. What additional funding is required to support the program (identity of source)

   Additional funding to establish the program with a strong positive reputation by supporting shared marketing/recruitment efforts, student scholarships, student attendance at conferences/professional engagements, student led research, student receptions, student awards/recognitions, and shared virtual laboratory space is expected to be provided in whole/part by the UMS and partnering institutions.

5. Lifetime of outside or independent funding and plan for how and when – becomes part of E&G budget

   N/A
VII. Program Evaluation

A. A post audit of an approved new program must be made after five years

Formative and summative assessments and evaluation of the program will be performed in accordance with existing UMS program review policies and NSA/DHS CAEIA/CD evaluation criteria.

Primary responsibility for program review will rest with the Academic Governance Board defined in the NSA/DHS CAEIA/CD application. The Chair of the Board will initiate and lead the review process in accordance with established policies.

The program review will benefit from interaction with industry and government. Examples of such interaction include industry representation on MCSC advisory boards, student involvement in industry/government sponsored Cybersecurity Internships, and frequent industry/government guest speakers.

Formative program information will be used as part of the two-year audit required for new programs by the UMS. The two-year report will examine enrollment data, student satisfaction, course grades, an exit survey, curriculum implementation, and industry representative/advisory board feedback, as well as an analysis of the cost-benefit projections. Another key part of the formative assessment/audit will be to evaluate the program’s progress and success at refining the alignment with the community colleges. The analysis will assess the successful connections made, the challenges, the needs, and the recommendations for making the program even more accessible to students throughout the state of Maine. The results of the audit will be reported to the Vice Chancellor for Academic Affairs as required, to the program advisory committee and to the Chief Academic Officers and Presidents of the Partnering Institutions.

Summative evaluation will include an analysis of enrollment, retention, and degree completion data and student and industry satisfaction surveys. This evaluation will reflect the experiences of students who have been able to complete the four-year cycle of classes and provide first-hand reflections on and assessments of their educational experience.

The first program review will be conducted during the fifth year of the program following the planned NSA/DHS 2019 re-recognition proceedings during the fourth year of the program. Regular reviews will be scheduled and conducted thereafter in accordance with UMS program review policies and consistent with NSA/DHS re-recognition timeline. The program review results will be
submitted to the Chief Academic Officers and Presidents of the Partnering Institutions, and after endorsement, the review will be submitted to the Vice Chancellor of Academic Affairs of UMS. Analysis of the program and its implementation will also be included in each Partnering Institutions’ application for continuing accreditation by New England Association of Schools & Colleges, Inc. (NEASC).
Submitted By (full-time faculty):

Raymond Albert  
Professor of Computer Science  
(Date)

Christopher Bennett  
Professor of Computer Science  
(Date)

Henry Felch  
Assistant Professor of Computer Science  
(Date)

Diana Kokoska  
Program Coordinator  
(Date)

George Markowsky  
Professor of Computer Science  
(Date)

Glenn Wilson  
Associate Research Professor  
(Date)
Approved By:

(UM Chief Academic Officer)  (Date)

(UM President)  (Date)

(UMA Chief Academic Officer)  (Date)

(UMA President)  (Date)

(UMF Chief Academic Officer)  (Date)

(UMF President)  (Date)

(UMFK Chief Academic Officer)  (Date)

(UMFK President)  (Date)

(USM Chief Academic Officer)  (Date)

(USM President)  (Date)
APPENDICES
References


B.S. in Cybersecurity Online Consortium – MOU
DRAFT - MEMORANDUM OF UNDERSTANDING\(^1\)

among

the Seven University of Maine System Institutions:

University of Maine
University of Maine at Augusta
University of Maine at Farmington
University of Maine at Fort Kent
University of Maine at Machias
University of Maine at Presque Isle
University of Southern Maine

for the Operation of the

Bachelor of Science in Cybersecurity Online Consortium Program

[ CURRENTLY UNDER DEVELOPMENT ]

---

\(^1\) Reference: This agreement is modelled on the University of Louisiana System Bachelor of Arts in Organizational Leadership Memorandum of Understanding
Sample of Support Letters
March 28, 2014

Evaluation Committee
Centers of Academic Excellence for Information Assurance Education Program
National Security Agency/Department of Homeland Security

Dear Ms. Mendez:

I write in support of the University of Maine System’s (UMS) application to be recognized as a Center for Academic Excellence in Information Assurance Education (CAE/IAE) by the National Security Agency and the Department of Homeland Security.

The World Wide Web has produced wondrous changes. But as an evolving frontier, it also is becoming more vulnerable to exploitation and attack. These vulnerabilities increase each day, as more and more activity finds its way onto cyber platforms. These dangers pose serious threats. Hackers could attack critical civilian infrastructures, such as electrical grids, transportation systems, and communications, affecting whole communities. Our military assets are at risk, too. If we do not build adequate protections for our federal networks and critical infrastructure, then the malicious hackers - civilian, military or terrorist - will exploit, attack, and destroy. As a nation, we must be prepared to aggressively and proactively meet this emerging global cyber threat.

UMS’ ‘UMS Center’ is attempting to ensure that students interested in preventing such threats have an institution prepared to educate them. The UMS Center is the only higher education entity in Maine that offers IA/CD-related degree programs and conducts IA/CD research. Currently, four of the University of Maine System’s seven Universities offer these programs and contribute to UMS Center’s mission to “provide the best possible IA/CD education, research and service to the citizenry of Maine and, in turn, the Nation.”

Since the UMS Center began in 2003, it has grown considerably. The University of Maine at Fort Kent (UMFK) established the first specialized Information Security concentration within the Bachelor of Science in Computer Applications degree program. Currently, a new Bachelor of Science in Information Technology degree program is being considered by the UMS Board of Trustees. The UMS hopes that graduates from this program will fill a gap in Maine’s IT workforce.

Maine is one of only seven states without a designated CAE institution. Therefore, I support UMS’ application and urge your most careful consideration, subject to all applicable laws and regulations. Thank you for your time and effort of behalf of the University of Maine System.

Sincerely,

Susan M. Collins
United States Senator
Evaluation Committee:
Centers of Academic Excellence for Information Assurance Education Program
National Security Agency / Department of Homeland Security

Dear Committee Members:

I am writing in support of the University of Maine System’s application to be recognized as a Center of Academic Excellence in Information Assurance Education (CAE/IAE) by the National Security Agency and the Department of Homeland Security.

Currently, Maine is one of just seven states without an institution designated as a CAE, and faculty from across the University of Maine system have come together to form an innovative program to ensure that students in our state have access to a high-quality cyber security curriculum. Individually, they have integrated an increased focus on security into their institutions’ information technology and computer science programs, and they plan to significantly expand on that success by creating a first of its kind system-wide Bachelor’s degree in cyber security. By sharing faculty expertise and resources, they will be able to provide students across Maine with access to top quality instruction, technology, and facilities. I am excited about the opportunities this presents for students in the University system, particularly for Maine’s many veterans of military service who are seeking educational and career opportunities that will build on their skills. I also appreciate the University’s efforts to ensure that the next generation of cyber security professionals is ready to address whatever threats the future brings.

The field of cyber security is one of critical importance to our nation, and I believe students and researchers in the State of Maine have a great deal to contribute to this emergent and ever-changing field. I enthusiastically support the University of Maine System’s application for a CAE/IAE designation, and I ask that you give them your full consideration.

Sincerely,

Chellie Pingree
Member of Congress
Evaluation Committee
National Centers of Academic Excellence in Information Assurance Education
National Security Agency/Department of Homeland Security

Dear Committee Members:

I am writing to offer my support for the University of Maine System’s (UMS) application to be recognized as a Center of Academic Excellence in Information Assurance Education (CAE/IAE) by the National Security Agency and Department of Homeland Security.

As you know, Maine is one of only a handful of states that does not have an institution of higher education designated as a CAE. Since 2003, UMS has made significant investments in information security education leading to the establishment of a Bachelor of Science Degree in Computer Applications with a concentration in Information Security at the University of Maine at Fort Kent (UMFK). Additionally, several UMS institutions offer information technology and security courses and certificate programs, including an Associate of Science in Information Security at UMFK, which is available to students throughout the state through distance education delivery modalities. UMS is also making efforts to enhance integration between institutions and eventually develop a system-wide degree in cyber security. These collaborative and comprehensive efforts to expand information technology and security education are truly a statewide undertaking, from the southern coast to the northern border with Canada, that not only benefit the students and institutions, but also the state’s economy and workforce.

These investments made by UMS directly benefit the state by producing qualified graduates who can help fill the gap in Maine’s information technology workforce and contribute to the health and wellbeing of businesses through information security. These programs also provide exciting educational and professional opportunities for our state’s large veteran population that includes many individuals who can build on existing capabilities and expertise. Additionally, through the Maine Cyber Security Cluster, which includes business, industry, government and UMS, students and faculty have been able to partner with the Maine State Police, the United States Coast Guard and the Maine Emergency Management Agency (MEMA), among other entities.

Recognizing UMS as a CAE/IAE would further the benefits of the existing programs and curriculum by providing additional grant opportunities for faculty and internship and employment opportunities for students and graduates, such as the federal government’s Scholarship For Service program. Further, designation as a CAE/IAE would solidify Maine’s status as a hub for information security research and education.
The United States Government and private companies are facing ever increasing threats from cyber attacks and data breaches, and we must do all we can to prepare our students and institutions of higher education in Maine and throughout the country to address this critical issue. That is why I offer my full support for the University of Maine System’s application to be recognized as a Center of Academic Excellence in Information Assurance Education and ask that you give it your full and fair consideration.

With warmest regards,

Michael H. Michaud
Member of Congress
Greetings,

I would like to help raise awareness to cyber security. The Internet plays a vital role in our lives and the future of our state and nation. Citizens, schools, libraries, businesses, and others use the Internet for a variety of tasks, including keeping up with family and friends, managing personal finance, performing research, enhancing education, and conducting business. Critical sectors of our state increasingly rely upon the Internet to support finance, telecommunications, energy, transportation, utilities, health care, and emergency response. Internet usage in Maine schools and institutions of higher learning enhances the education of our youth by providing increased access to educational and research materials.

Unfortunately, our Internet infrastructure faces an increased threat of cyber-attack, with the potential for significant losses due to theft and fraud. In Maine, a multi-stakeholder Cyber Security initiative continues to bring together local industry, institutions of higher learning, the State, the Maine Technology Institute, and others to combat cyber threats. While partnerships between government and industry experts are important, maintaining Internet security is a shared responsibility in which each of us has a critical role to play. The U.S. Department of Homeland Security, the Multi-State Information Sharing & Analysis Center, the National Association of State Chief Information Officers, and the National Cyber Security Alliance have all declared October as the National Cyber Security Awareness Month. It is important for Maine citizens to use this month to learn more about how they can help combat cyber security threats.

I, Paul R. LePage, Governor of the State of Maine, encourage all Maine citizens to be aware of cyber security and ways to prevent a cyber attack.

Sincerely,

Paul R. LePage
Governor
March 16, 2012

Betsy Biemann
President
Maine Technology Institute
8 Venture Avenue
Brunswick Landing
Brunswick, ME 04011

Dear Ms. Biemann:

This letter represents a commitment by Tilson Technology Management to participate as an Advisory Board member to the University of Southern Maine’s Cluster Initiative Program Award project entitled Maine Cyber Security Cluster (the “Program”). Tilson is excited to be a member of this important group and urge MTI to support funding of the Program.

Tilson is an entrepreneurial, Maine-based technology company with a specialized consulting practice in information security. Our team provides services across the complete range of information security – from security architecture design and implementation to regulatory compliance programs. Tilson’s clients in this area include government agencies, large multi-national corporations, and e-commerce companies. Tilson prides itself on delivering exceptional quality in its services through its impressive team of experts.

Over the three-year period of the proposed MTI grant, Tilson has approved 120 hours in personnel time to participate on the Board of Advisors and the various working groups and activities to be developed by the proposed Program. We estimate that this is valued at $24,000 in the form of salaries, use of equipment, materials or other services devoted to this project.

The proposal includes a provision to develop the Program’s business plan by the end of August 2012. It is our intention to work closely with the Program participants as this business plan is developed to ensure the objectives of the Cluster Initiative Program are met, including work force development and establishing a base for economic growth in the State. Based upon the Program’s proposal and our understanding of its intent, we also will work in good faith to identify fee-for-service arrangements under which our company could make use of the Program’s proposed Cyber Security Laboratory. Based upon our understanding of the Program proposal, this laboratory has significant economic development potential for the State.

On behalf of Tilson, I ask that you seriously consider this proposal. Thank you for your time in effort in advancing the cause of economic development in the State.

Sincerely,

Ande Smith
Chief Operating Officer
Email and Mail

March 12, 2012

Betsy Biemann
President
Maine Technology Institute
8 Venture Avenue
Brunswick Landing
Brunswick, ME 04011

Dear Ms. Biemann:

This letter represents a commitment by State of Maine, Office of Information Technology to participate as an Advisory Board member to the University of Southern Maine’s Cluster Initiative Program Award project entitled Maine Cyber Security Cluster (the “Program”).

As with all large organizations, we here at the Information Technology Department for the State of Maine must be consistently vigilant regarding the ever-evolving cyber threats. We have cyber security staff dedicated to this issue, and we firmly believe in working with other organizations and the University System to understand best practices.

Over the three-year period of the proposed MTI grant, my company has approved 120 hours in personnel time to participate on the Board of Advisors and the various working groups and activities to be developed by the proposed Program.

The proposal includes a provision to develop the Program’s business plan by the end of August 2012. It is our intention to work closely with the Program participants as this business plan is developed to ensure the objectives of the Cluster Initiative Program are met, including work force development and establishing a base for economic growth in the State. Based upon the Program’s proposal and our understanding of its intent, we also will work in good faith to identify fee-for-service arrangements under which our company could make use of the Program’s proposed Cyber Security Laboratory. Based upon our understanding of the Program proposal, this laboratory has significant economic development potential for the State.

On behalf of the State of Maine, Office of Information Technology, I ask that you seriously consider this proposal. Thank you for your time in effort in advancing the cause of economic development in the State.

Sincerely,

James R. Smith
Chief Information Officer

cc: Glenn Wilson, Associate Professor of Technology, Senior Research Scientist

Phone: (207) 624-8800/(207) 624-9494
Fax: (207) 287-4563
TTY: (207) 629-9015
www.Maine.gov
23 March 2012

Betsy Biemann, President
Maine Technology Institute
8 Venture Avenue
Brunswick Landing
Brunswick, ME 04011

Dear Ms. Biemann:

This letter represents a commitment by LANCO Assembly Systems to participate as an Advisory Board member to the University of Southern Maine’s Cluster Initiative Program Award project entitled Maine Cyber Security Cluster (the “Program”).

As LANCO continues to become more International, its ability to communicate quickly and securely across continents is essential to its success. Therefore, protection of information, as it is transmitted electronically to different places in the globe, is of paramount importance. It is in our best interest to help see that students are trained in cyberspace security so that they may enter the workforce and apply this knowledge to help Maine companies like LANCO protect their proprietary property.

Over the three-year period of the proposed MTI grant, LANCO is committed to donate at least 120 hours in personnel time to participate on the Board of Advisors and the various working groups and activities to be developed by the proposed Program. We estimate that this is probably worth $10,000 in the form of salaries, use of equipment, materials or other services devoted to this project.

The proposal includes a provision to develop the Program’s business plan by the end of August 2012. It is our intention to work closely with the Program participants as this business plan is developed to ensure the objectives of the Cluster Initiative Program are met, including work force development and establishing a base for economic growth in the State. Based upon the Program’s proposal and our understanding of its intent, we also will work in good faith to identify fee-for-service arrangements under which our company could make use of the Program’s proposed Cyber Security Laboratory. Based upon our understanding of the Program proposal, this laboratory has significant economic development potential for the State.

On behalf of LANCO Assembly Systems, I ask that you seriously consider this proposal. Thank you for your time in effort in advancing the cause of economic development in the State.

Best regards,

[Signature]

Thomas A. Zuck
Chairman of the Board
Betsy Biemann
President

Maine Technology Institute
8 Venture Avenue
Brunswick Landing
Brunswick, ME 04011

Dear Ms. Biemann:

This letter represents a commitment by Unum Group to participate as an Advisory Board member to the University of Southern Maine’s Cluster Initiative Program Award project entitled Maine Cyber Security Cluster (the “Program”).

The importance of safeguarding Unum’s information and that of our customers has increased significantly in recent years as we have become increasingly dependent on information technology as well as the Internet for conducting business. As the threat landscape continues to change rapidly so does the need for a strong cyber security program. It’s through this type of program that we implement the processes and technology to ensure that we maintain the availability, integrity and the confidentiality of the information that we create and maintain.

Over the three-year period of the proposed MTI grant, my company has approved 60 - 120 hours in personnel time to participate on the Board of Advisors and the various working groups and activities to be developed by the proposed Program. We estimate that this is valued at $6,700.00 - $11,400 in the form of salaries, use of equipment, materials or other services devoted to this project.

The proposal includes a provision to develop the Program’s business plan by the end of August 2012. It is our intention to work closely with the Program participants as this business plan is developed to ensure the objectives of the Cluster Initiative Program are met, including work force development and establishing a base for economic growth in the State. Based upon the Program’s proposal and our understanding of its intent, we also will work in good faith to identify fee-for-service arrangements under which our company could make use of the Program’s proposed Cyber Security Laboratory. Based upon our understanding of the Program proposal, this laboratory has significant economic development potential for the State.

On behalf of Unum Group, I ask that you seriously consider this proposal. Thank you for your time in effort in advancing the cause of economic development in the State.

Sincerely,

Lynda R. Fleury, CISM
Unum – VP Chief Information Security Officer
1 Fountain Square
Chattanooga, TN 37402

Unum is a registered trademark and marketing brand of Unum Group and its insuring subsidiaries.
Betsy Biemann  
President  
Maine Technology Institute  
8 Venture Avenue  
Brunswick Landing  
Brunswick, ME 04011  

March 26, 2012  

Dear Ms. Biemann:

This letter represents a commitment by S.D. Warren Company d/b/a Sappi Fine Paper North America ("Sappi") to participate as an Advisory Board member to the University of Southern Maine’s Cluster Initiative Program Award project entitled Maine Cyber Security Cluster (the "Program").

Reliable networks and computing systems provide a firm foundation for a 21st century company, and cybersecurity supports this endeavor. Sappi takes very seriously the threats of data security and control, both from an internal and external perspective. Development of the program would provide an additional avenue of training and professional development for our staff as well as provide a potential pool of skilled information technology resources for the region and beyond.

Over the three-year period of the proposed MTI grant, Sappi has approved 120 hours in personnel time to participate on the Board of Advisors and the various working groups and activities to be developed by the proposed Program. We estimate that this is valued at $5,500 (based on 3 weeks) in the form of salaries, use of equipment, materials or other services devoted to this project.

The proposal includes a provision to develop the Program’s business plan by the end of August 2012. It is our intention to work closely with the Program participants as this business plan is developed to ensure the objectives of the Cluster Initiative Program are met, including work force development and establishing a base for economic growth in the State. Based upon the Program’s proposal and our understanding of its intent, we also will work in good faith to identify fee-for-service arrangements under which our company could make use of the Program’s proposed Cyber Security Laboratory. Based upon our understanding of the Program proposal, this laboratory has significant economic development potential for the State.

On behalf of Sappi I ask that you seriously consider this proposal. Thank you for your time in effort in advancing the cause of economic development in the State of Maine.

Sincerely,

Anne Ayer  
VP, Corporate Development & CIO  
Sappi Fine Paper North America
Betsy Biemann  
President  
Maine Technology Institute  
8 Venture Avenue  
Brunswick Landing  
Brunswick, ME 04011

Dear Ms. Biemann:

This letter represents a commitment by Kepware Technologies to participate as an Advisory Board member to the University of Southern Maine’s Cluster Initiative Program Award project entitled Maine Cyber Security Cluster (the “Program”).

Kepware Technologies is a software development firm that specializes in the area of communications products for the global industrial automation market. This market is comprised of automotive, packaging, pharmaceutical, food and beverage, water and waste water management, oil & gas, power, among many other sectors where the need for secure and reliable transmission of data is critical to process control. These markets require 24 by 7 operations where any interruption can cost millions in downtime and errors can cause loss of life. It is imperative that our software solutions meet the security requirements of our customers and believe the deliverables of this program will provide us with future employees skilled in the area of security, as well as a local lab to run a wide variety of tests that don’t affect our corporate production environment.

Over the three-year period of the proposed MTI grant, my company has approved 120 hours in personnel time to participate on the Board of Advisors and the various working groups and activities to be developed by the proposed Program. We estimate that this is valued at $17,500.00 in the form of salaries, use of equipment, materials or other services devoted to this project.

The proposal includes a provision to develop the Program’s business plan by the end of August 2012. It is our intention to work closely with the Program participants as this business plan is developed to ensure the objectives of the Cluster Initiative Program are met, including work force development and establishing a base for economic growth in the State. Based upon the Program’s proposal and our understanding of its intent, we also will work in good faith to identify fee-for-service arrangements under which our company could make use of the Program’s proposed Cyber Security Laboratory. Based upon our understanding of the Program proposal, this laboratory has significant economic development potential for the State.

On behalf of Kepware Technologies, I ask that you seriously consider this proposal. Thank you for your time in effort in advancing the cause of economic development in the State.

Sincerely,

Tony Paine  
Kepware Technologies – President & CEO
Faculty Curriculum Vitae
RAYMOND T. ALBERT
Curriculum Vitae
P.O. Box 26
Eagle Lake, Maine 04739
(207) 444-4544 (home)
Telephone: (207) 834-7696
e-mail: ralbert@maine.edu

Education:
Online Teaching Certificate (SLOAN-C Institute), Newburyport, Massachusetts, August 2012;

Post-Graduate Certificate (CS), Purdue University, West Lafayette, Indiana. August, 2003;
Program: Information Assurance/Security (Computer Science)

Doctor of Philosophy, University of Florida, Gainesville, Florida. December, 1996;
Concentrations: Curriculum and Instruction
                Educational Media and Instructional Design
                Bilingual/Multicultural Education
Grade point average: 4.0/4.0
Dissertation: Relationships among Bilingualism, Critical Thinking Ability, and Critical Thinking Disposition of Baccalaureate Nursing Students
Doctoral supervisor: Lee J. Mullally, Ph.D. Department of Curriculum and Instruction, College of Education, University of Florida.

Master of Science, University of Vermont, Burlington, Vermont. 1986;
Major: Computer Science
Grade point average: 3.5/4.0
Comprehensive/Theses: Concurrency Construct Analysis of the Synchronizing Resources (SR) Programming Language,
                        Analysis of Error Propagation and Recovery in Concurrent Environments.

Bachelor of Arts, University of Maine, Fort Kent, Maine. 1983;
Field: Mathematics/Science
Grade point average: 3.1/4.0

Relevant Graduate Study:
Intro. & Advanced Information Assurance
Intro. & Advanced Operating Systems
Intro. & Advanced Computer Architectures
Intro. & Advanced Programming Languages
Design & Development of Educ. Media
Production and Utilization of Educ. Media
Educ. Television Design and Production
Computer Security
Digital Computer Design
Algorithm Analysis
Real Time Systems
Instr. Message Design
Interactive Video
Ed. Psych. Learning Theory
Cryptography
Theory of Comp.
DBMSs
Data Structures
Instr. Development
Animation/Graphics
Working Knowledge of Programming Languages:

C (50,000+ lines of code), Java, Python, Visual Basic. Also experience with: Actor, Ada, Alice, Algol68, ASP, C++, C#, COBOL, Delphi 2, FORTRAN, HyperCard, JavaScript, Lisp, MASM, Pascal, Perl, and SNOBOL.

Teaching Experience:

**Sept. 2004 - Present**  
Program Coordinator for Computer Applications and Information Security, University of Maine, Fort Kent, Maine.  
Responsibilities include oversight and management of Computer Applications and Information Security degree programs. This program has two full-time faculty and six adjunct faculty.

**Sept. 2004 - Present**  
Professor of Computer Science, University of Maine, Fort Kent, Maine.  
Responsibilities as cited under Associate Professor of Computer Science (see below).

**June 2005 – Sept. 2009**  
Natural/Behavioral Sciences Division Chair, University of Maine, Fort Kent, Maine.  
Responsibilities included oversight and administration of division budgets; approval of course schedules and faculty assignments, coordination of the effective assessment of all programs and of student outcomes; providing support, guidance and objective feedback to all division personnel. The division consisted of 19 full-time and 15 part-time faculty, and 3 staff members in more than 8 different discipline areas with a combined $1.9M operating budget.

**Sept. 2001 – Sept. 2010**  
Adjunct Professor, Nova Southeastern University, Graduate School of Computer and Information Sciences, Fort Lauderdale, Florida. Responsibilities included teaching of graduate level Information Security and Database Systems courses among others.

Associate Professor of Computer Science, University of Maine, Fort Kent, Maine. Responsibilities as cited under Assistant Professor of Computer Science (see below). Awarded tenure September 1, 1996. Contributing member of Chancellor's Information Technology Task Force. Delivered full course load from a distance (Ohio) to locally situated (Maine) students during 1998-1999 academic year using mixed media (Internet, VHS, telephony). Have offered following courses:
Bachelor of Science in Cybersecurity Program Proposal

Introduction to Computers
Intro. to Information Technology
Introduction to Programming
Computer Organ./Assembly Lang.
Operating Systems
Systems Analysis and Design
Information Assurance & Security
Network Security
Computer Prog. I & II - C
Computer Prog. I & II - C++

Programming Languages
Data Structures
Advanced Prog. Using Pascal
Database Management Systems
Local Area Networks
Networking
Cryptography
Computer Prog. I & II – COBOL
Computer Prog. I & II – FORTRAN
Computer Prog. I & II – VB

Committees served:

UMS Technology Assessment Comm.
Presidential Search Committee
Faculty Chair
Strategic Planning Steering Comm.
Chancellor's Telecomm. Working Group
Academic Computing Committee
Faculty Development Committee
Desktop Publishing Comm.
Quad-campus UNIX System Users Group

President’s Cabinet
Fac. Rep. to UMS Board of Trustees
Peer Review Committee
Academic Council
Faculty Secretary
Innovative Teaching Fund Comm.
Software Eval./Selection Comm.
Computer Center Advisory Comm.
AFUM Union Representative
Chancellors Task Force on Telecommunication and Information Technology

Sept. 1989 - Dec. 1996 Assistant Professor of Computer Science, University of Maine, Fort Kent, Maine. Responsibilities included teaching of 12 credit hour Computer Science course load per semester (two semester year). Also involved in student academic advising, faculty committee work, and degree program reviews. Have regularly managed direct studies, internships and have carried a credit-hour overload to accommodate student and campus needs. Offered COSK 100 Introduction to Computers course statewide via the University of Maine Interactive Television System during both fall and spring semesters beginning with fall semester 1991. Educational leave of absence granted from 09/01/89 through 08/31/90. Sabbatical granted from 9/1/93 through 9/1/94 followed by a second educational leave from 9/1/94 through 9/1/95.


Sept. 1993 - May 1995 Graduate Teaching Assistant, University of Florida, Gainesville, Florida. Responsibilities included provision of instructional design and development assistance to liberal arts faculty implementing large-scale multimedia presentations. Efforts conducted through the University of Florida, Office of Instructional Resources (OIR).

Sept. 1991 - Dec. 1992 Assistant Professor of Computer Science, University of Maine at Fort Kent, Maine.
Upon request, offered COSK 100 Introduction to Computers course over the Education Network of Maine (formerly Instructional Television system of Maine). Course offered statewide over distance education system consisting of over 75 receive sites. Developed several innovative instructional/assessment tools designed to support and enhance remote communication between students and faculty.

**Jan. 1987 - July 1989**  
**Instructor of Computer Applications, University of Maine, Fort Kent, Maine.**  
Responsibilities included teaching of four Computer Science courses per semester (two semester year). Also student academic advising and faculty committee involvement. One half-release time granted during first academic year for implementation of campus computer ISN network and 3B2/400 minicomputer system. Joint fiscal academic computing responsibility during academic years 1987 - 1988. Joint participation in design and implementation of Computer Applications Baccalaureate degree program. Joint participation in design and implementation of inter-campus Computer Applications outreach program developed for Loring Strategic Air Command Base. Co-developed the Academic Computing Environment (ACE) technology infrastructure specification for UMFK campus.

**Sep. 1984 - Dec. 1986**  
**Teaching Fellow, University of Vermont, Burlington, Vermont.**  
Duties included teaching of two lab sections of CS-11 (Computer Programming) course. General responsibilities included administration of lectures, programming assignments, and quizzes as well as student counseling support provided through several office hours planned during each week.

**Professional Experience:**

**Jan. 1998 – June 2007**  
**Managing Partner and CEO, QualityQuest, L.L.C., Eagle Lake, Maine.**  
QualityQuest, L.L.C., a New England based company, is a pioneer in the field of electronic surveying and evaluation. The services it offers utilize the latest server-side software technology available, while taking advantage of the existing network infrastructure already in place in most college campuses and companies nation-wide. Through its innovative approach to information collection, analysis and reporting, its premier service, Excel-A-Rate℠ provides clients a cost-effective turn-key solution to Internet-based online data collection and reporting.

**June 1989 - Aug. 1990**  
**Software Quality Engineer, NASA Johnson Space Center, Houston, Texas.**  
Responsibilities included analysis of contractor software development methodologies including recommendations for process improvement, problem trending, discrepancy report/waiver/deviation/change request review and disposition, general configuration management involvement, formal test procedure review and test witnessing, major scheduled milestone review participation, software product assurance standard development participation. Specific program of emphasis was the SSE (Software Support Environment) for SSFP (Space Station Freedom Program).


Jun. 1983 - Aug. 1984  **Community Development Director**, Town of Eagle Lake, Eagle Lake, Maine. Responsibilities included both fiscal and administrative control over 1983-1984 federal Community Development Block Grant (C.D.B.G.) awarded to town. Grant funds in excess of $360,000 were primarily targeted for use in low/moderate income house rehabilitation projects throughout the entire community.

---

**Selected Presentations:**


Co-presenter.  **Approaches to Blended (‘Hybrid’) Learning within the University of Maine System**, First New England Regional SLOAN-C Conference on collaboration, collegiality, and community among online educators, October 2009.

Presenter.  **The ‘U’ in Information Security**, Association of Small Computer Users in Education (ASCUE) 2009 conference on academic and administrative technology issues and innovation in higher education.
Bachelor of Science in Cybersecurity Program Proposal


Accepted to present but unable to attend. Computer-based Course Tools for Distributed Education. Information Technology Issues in Community Health (ITCH) international conference, University of Victoria, December 1992.

Selected Publications:


**Selected Reviews:**  
Invited review of “From Novice to Expert: Harnessing the Stages of Expertise Development in the Online World”, article submission to Association of Small Computer Users in Education (ASCUE) 2009 conference on academic and administrative technology issues and innovation in higher education.

Invited review of “The Effectiveness of Podcasting on Achievement in Principles of Accounting”, article submission to Association of Small Computer Users in Education (ASCUE) 2009 conference on academic and administrative technology issues and innovation in higher education.

Invited review of “Identification, Causes, and Prevention of Identity Theft”, article submission to Association of Small Computer Users in Education (ASCUE) 2009 conference on academic and administrative technology issues and innovation in higher education.

Invited review of “Capture Everything: Architecting a set of technologies and policies to support enterprise video capture” conference proposal submission to Future Trends and Technologies track of the EDUCAUSE 2009 Annual Conference on the best thinking in higher education IT.

Invited review of “It’s an enrollment world: How technology can help” conference proposal submission to Future Trends and Technologies track of the EDUCAUSE 2009 Annual Conference on the best thinking in higher education IT.

Invited review of “PHISHING the PHISHER using Web Bugs and HoneyTokens to Investigate the Source of PHISHING Attacks”, article submission to Hawaii International Conference on System Sciences (HICSS) 2008.


Focus group participant. Opinions sought regarding major technology issues and how they affect self and institution, October, 2002.

SimNET XPert - Office XP Assessment Software. Published by McGraw Hill. April, 2002.
Creative Works:  “Your Password, Your Identity, Your Privacy” instructional unit. This unit was selected by the EDUCAUSE Security Task Force for international distribution during Fall, 2004. As part of National Cyber Security Awareness Month (http://www.staysafeonline.info/home-news.html), the Security Task Force compiled a CD that contains Cybersecurity Awareness Resources for the Higher Education Community. The availability of the CD was announced during the 2004 EDUCAUSE Live Event on "Campus and National Approaches to Cybersecurity Awareness." An archive of the event is available at http://www.educause.edu/LIVE0411. Every attendee of the EDUCAUSE Annual Conference in Denver received a CD as part of their registration materials.

Database-backed Website Project. University of Maine at Fort Kent, Summer 2001 – Fall 2001. As co-recipient of a University of Maine System Trustee Professorship I designed and implemented a database and associated website to allow visitors to learn more about the UMFK Lichen Research Program containing information on more than 9000 lichen specimens. Visit http://130.111.186.6/ (the site is currently awaiting DNS assignment) for more details.


PAC-MAINE software application designed to address governor's request for innovative methods for raising students aspirations within the state of Maine. PAC-MAINE initially distributed to all public/private secondary education guidance and counseling offices throughout New England. Subsequent requests for PAC-MAINE have come from as far away as California. PAC-MAINE has been showcased by BBS Press Service, which serves 235 electronic bulletin boards in the U.S., Canada and overseas. Newsday requested information on PAC-MAINE, and literature was forwarded to the software review editors of 100 national computer magazines and 250 educational publications. Initially designed to address low student educational aspirations within the state, PAC-MAINE has spread across the entire country and Canada. Congratulatory letters from Governor John McKernan, Commissioner of Education Eve Bither, and University of Maine System Chancellor Robert Woodbury, available upon request.

UMS/ITV System Integration Prototype designed to integrate and improve testing, evaluation and grading via interactive television system of Maine. Developed as part of Annenberg/CPB grant awarded during 1991-1992 academic year. Continued development of prototype into full-scale system serving all ITV receive sites as part of second successful Annenberg/CPB grant awarded during 1992-1993 academic year. Presentations made at EDUCOM '92 and Computer on Campus national conferences.
OFACET (Online Faculty Evaluation Tool) prototype designed to address confidentiality and other concerns of University of Maine at Fort Kent administration, faculty and student concerns regarding faculty evaluation by students. Application development discontinued during sabbatical/educational leaves 1993-1995, development of full-scale application evolved into Internet-based Excel-A-Rate™ service.

GRE Word Study Software application designed to assist UMFK community in preparation for Verbal component of Graduate Record Examination. Application development discontinued during sabbatical/educational leaves 1993-1995, further development of full-scale application currently in progress.

UMSServe Web Site specification development.

Honors:

NIST sponsored participation in “4th Annual Shaping the Future of Cybersecurity Education ‘Navigating the National Cybersecurity Education Interstate Highway’ Workshop” (September 16-19, 2013).

NIST sponsored participation in “3rd Annual Shaping the Future of Cybersecurity Education ‘Connecting the Dots in Cyberspace’ Workshop” (October 30 – November 1, 2012).

Maine Innovation Engineering Leadership Institute. Selected to participate in training to become eligible to teach courses in UMS Innovation Engineering minor and graduate certification offerings (March 5-7, 2012).

Homeland Security Faculty Development Workshop. Selected as one of only 30 university faculty members nationwide offered to participate in this program. The program was sponsored by the University and Agency Partnership Initiative (UAPI), a program of the Naval Postgraduate School Center for Homeland Defense and Security (CHDS). The purpose of the program was to bring together institutions nationwide dedicated to advancing homeland security education and increase the number and diversity of students receiving homeland security education, accelerate the establishment of high-quality academic programs, and provide opportunities for collaboration that create an intellectual multiplier effect that furthers the study of homeland security. Summer 2011.

Grant partner ($10,000 component of $123,720) for “Advancing Higher Education through Excellence in Online and Technologically Enhanced Instruction: Implementing an On-campus Teaching and Technologies Laboratory”. Specifically for networking technologies in support of new proposed Associate of Science in Information Security degree). AY 10/11.

Principal Investigator for ($30,000) multi-campus collaborative project entitled “Cyber Defense Competitions as a Method to Raise Awareness and Interest of High School Students in University of Maine System STEM programs”. AY 10/11.


Invited by Educational Testing Service (ETS) to serve as reader for Advanced Placement (AP) – Computer Science exams

Principal Investigator for ($30,000) multi-campus collaborative project entitled “Cyber Defense Competitions as a Method to Raise Awareness and Interest of High School Students in University of Maine System STEM programs”. AY 09/10.

Co-recipient of University of Maine System Trustee Professorship ($12,500) for design and implementation of “A Prototype Wildlife Detection System for Animal-Vehicle Collision (AVC) Prevention” a project to build upon and extend research in this area by designing and implementing a prototype wildlife detection system based on an “intelligent” multi-sensory-node network design that can reliably detect wildlife in the roadway while simultaneously preventing the production of false positive alerts. AY 07/08.

Information Assurance Education Graduate Certificate Program. Selected, with Professor Gauvin, as two of only 25 college and university faculty members nationwide offered to participate in this program. The program was sponsored by the National Security Agency (NSA) and delivered by the Purdue University Center for Education and Research in Information Assurance and Security (CERIAS). Program objective was to assist NSA with their goal of filling the need for trained faculty to develop and teach Information Assurance Program at colleges and universities across the nation. Summer 2003.


Innovative Teaching Fund grant ($1,500) during academic year 1998-1999 for design and implementation of a distance delivery model and assessment methodology for instruction delivered from a distance to locally situated computer students. Courses delivered to local Maine campus students from Ohio during academic year.

Innovative Teaching Fund grant ($1,440) during academic year 1997-1998 for design and implementation of student technological intern program to enhance the quality and effectiveness of Computer Applications majors’ educational experience and to
augment the existing pool of skilled human resources available for the completion of on-campus computer projects.

University of Maine System Tri-campus Consortium grant ($7,300) awarded to support continued beta testing and piloting of a Web-based online faculty/course evaluation system during Spring 1997 semester.

Faculty Development grants averaging $1,500 per year since 1987 to support attendance and participation in international conferences (e.g., EDUCOM, EDUCAUSE).

United States Department of Education, Office of Bilingual and Minority Language Affairs bilingual/multicultural fellowship ($20,000) during academic years 1994 - 1996.

UMFK Innovative Teaching Fund ($3,025) for Web-based assessment tools.


Awarded undergraduate computer science teaching fellowships at the University of Vermont, Burlington, during academic years 1984 - 1986.

Pinkham Family Trust Fund Scholarship ($7,000) 1984.

Community Service:

Civil Air Patrol (033 – County composite squadron based at Caribou, ME) serve as Transport pilot and Aerospace Education Officer (2004-present). Hold rank of Major. Conduct fire patrol flights throughout summer months.

Association of Small Computer Users in Education (ASCUE) 2009 Program Committee (2000).

EDUCAUSE Annual Conference proposal evaluator (2009).

Educational Testing Service (ETS) reader for Advanced Placement (AP) – Computer Science exams (invited 2008).


EDUCAUSE Annual Conference proposal evaluator (2005).


Offered computer consulting regularly to local departments, organizations and businesses since 1990.

Offered "Computers - Why all the Fuss?" course to summer Elderhostel program participants (1991).

Offered three day ENABLE integrated software seminar to county National Guard officers, (Spring 1988).

Offered following workshops to community residents and businesses (Spring 1988): Introduction to Microcomputers, Intro. DOS, and Intermediate DOS.

Co-development of Lichenological database using the SMART integrated software system.


St. Mary's Reader (1988 - Present).


Software Forum held for regional secondary and post-secondary mathematics/science education group (Spring 1989).

Membership:
IEEE (2009-).
EDUCAUSE (1999-).
Round Table Group (Expert Witness Search and Referral firm) (2008-).
Phi Delta Kappa (1994-).
Civil Air Patrol (2004-).
Association for the Advancement of Computing in Education (2003-).
Association for Educational Communications and Technology (1994-).
Upsilon Pi Epsilon national computer science honor society (1986-).
Association of Computing Machinery (1988-).
Associated Faculties of the University of Maine System (1987-).
Maine State Teachers Association (1987-).
Maine Municipal Association (1979-).
Aircraft Owners and Pilot Association (1996-).
Certifications:  
EC-Council Certified Ethical Hacker (CEH - ECC966439) (2013-)
SLOAN-C Online Teaching Certified-specialized in Blended Learning (2012-)
CompTIA Security+ (COMP001020100212) (2010-) Verifiable by entering code
FAA (Airplane Single Engine Land) rated Private Pilot (1990-)
Maine State Certified Scuba Diver (1988 -)
Certified Class II (CDL) Driver (1979-)
Maine State Licensed Guide (1978-)

References:  
Furnished upon request.
CURRICULUM VITAE

David A. Briggs, Ph.D.
Professor, Computer Science Department
220 Science Building
University of Southern Maine
Portland, Maine 04104-9300
(207) 780 4723
E-mail: briggs@usm.maine.edu

I. Personal Data
   A. Education
      B. A. 1975 History Swarthmore College
      M. S. 1984 Computer Science University of Massachusetts
      Ph. D. 1988 Computer Science University of Massachusetts
      Advisor: Professor Robert Moll

   B. Experience
      1976 - 1977 Peace Corps Volunteer
      1981 - 1982 Teaching Assistant/Lecturer, Introductory Programming Course, University of Massachusetts
      Fall 1982 Instructor, Theory of Computation, Smith College
      Spring 1983 Research Assistant, designed kernel primitives for a distributed operating system, University of Massachusetts.
      Fall 1983 Teaching Assistant, Data Structures, University of Massachusetts
      Spring 1984 Designed and implemented a data base for a private company
      1984 - 1990 Assistant Professor, Computer Science, University of Southern Maine
      1991 – present Associate Professor, Computer Science, University of Southern Maine

II. Grants and Awards
   1971 National Merit Scholar
   1986-1987 Supported Leave of Absence University of Southern Maine
   Graduate School Fellowship, University of Massachusetts
   Star Award for Excellence in DBMS Research Relational Technology Institute
   Summer Faculty Fellowship, University of Southern Maine
   1992 Supported Sabbatical Leave, University of Southern Maine
   2003-2004 Supported Sabbatical Leave, University of Southern Maine
   2008-2009 Maine Geolibrary Geoportal Project

III. Journal Publications

IV. Papers in Springer-Verlag Lecture Notes in Computer Science


V. Conference Presentations


VI. Unpublished Papers


VII. Courses Taught

• COS 160 Structured Problem Solving: Pascal
• COS 161 Algorithms in Programming
• COS 280 Discrete Mathematics
• COS 285 Data Structures
• COS 420 Object-oriented Design
• COS 430 Software Engineering
• COS 457 Database Systems
• COS 469 Compiler Construction
• COS 472 Artificial Intelligence
• COS 480 Theory of Computation
• COS 485 Design of Computing Algorithms
• COS 558 Database Systems
• COS 569 Compiler Construction
• COS 570 Special Topics: Parallel Processing
• COS 570 Special Topics: Functional Programming
• COS 570 Special Topics: The XML Data Model
• COS 573 Formal Methods in Software Engineering
• COS 582 Design and Analysis of Algorithms
CURRICULUM VITAE
Henry J. Felch, DCS

- Over 8 years’ experience teach computer science and Information Technology courses on the Baccalaureate, Master and Doctoral level, formats have include live course, hybrid classes, online classes, and interactive television.
- A results driven leader who is committed to excellence. An astute mentor and visionary leader, who takes great pride in his work.
- Over 20 years of training soldiers in the Army, proven track record in development of highly functional teams, delivering bottom-line results.
- Highly organized and detail-oriented leader possessing superb mentoring and training skills.
- An adaptable leader, innovative problem solver and brilliant resource manager. Detail-oriented, yet extremely versatile.

EDUCATION

DOCTORATE OF COMPUTER SCIENCE (2009)
Colorado Technical University, Colorado Springs, Colorado
Dissertation: An Evaluation of a Network Defense Strategy Combining Traditional Methods with Anomaly Detection

MASTER OF SCIENCE COMPUTER SCIENCE (2004)
Colorado Technical University, Colorado Springs, Colorado
(major in computer systems security)

MASTER OF SCIENCE COMPUTER SCIENCE (2002)
University of Phoenix, Colorado Springs, Colorado
(major in computer information systems)

MASTER OF EDUCATION (1998)
University of Louisville, Kentucky
Bachelor of Science in Cybersecurity Program Proposal

(major in occupational training and development with a concentration in instructional technology)

BACHELOR OF SCIENCE (1997)

University of Louisville, Kentucky

(major in training and development)

ASSOCIATE OF ARTS, COMPUTER STUDIES (1991)

University of Maryland, University College, College Park, Maryland
Classes taught have been on ground, hybrid, online, and ITV (interactive Television classes).

Classes taught

- Introduction to Computer Science (Fall 2011, Spring 2012, Fall 2012, Spring 2013, Fall 2013, Spring 2014)
- Introduction to Computing (Spring 2012, Fall 2012, Spring 2013, Fall 2013, Spring 2014)
- Networking Concepts (Spring 2012, Fall 2012, Spring 2013, Fall 2013, Spring 2014)
- Advanced Networking (Spring 2014)
- Network Security (Spring 2012, Spring 2013)
- Database Design and Management (Fall 2011, Fall 2012)
- Introduction to Digital Security (Summer 2012)
- System Analysis and Design (Fall 2012, Fall 2013)
- Systems Forensics I (Summer 2013)
- Introduction to Information Security (Summer 2013, Spring 2014)
- Security Risk Management (Fall 2013)
- Network Defense I (Spring 2014)
- Information Security Management (Spring 2014)
- Internship Mentor for 6 students (Spring 2012, Summer 2012)

Adjunct Professor, Colorado Technical University, Colorado Springs, Colorado, January 2006 – Present

Classes taught have been on ground, hybrid classes (combination of on ground and online), and online classes.

Undergraduate Classes Taught

- Client-Server and Network Administration (Winter 2009)
- Database Applications with Microsoft Access (Summer 2009)
- Information Technology Architecture (Spring 2007)
- Introduction to IT (Winter 2006, Spring 2006, Fall 2007, & Spring 2008)
Bachelor of Science in Cybersecurity Program Proposal

- Introduction to Unix (Winter 2007 & Spring 2008)
- Spreadsheet Applications (Fall 2007 & Summer 2008)

Master Level Classes Taught

- Computer Security Fundamentals (Summer 2006)
- Database Systems (Fall 2010, Fall 2011, & Winter 2012)
- Foundations in Information Technology (Summer 2007, Winter 2009, & Summer 2009)
- Information Technology Systems Development (Summer 2008 & Summer 2010)
- IT Systems Implementation (Summer 2008, Spring 2010, & Winter 2010)
- Network Security (Spring 2007, Fall 2007, & Summer 2010)
- Networking and Telecommunications (Summer 2007, Fall 2007, Fall 2009, & Winter 2010)
- Software Design (Summer 2008)

Adjunct Professor, Colorado Technical University Institute for Advanced Studies, Colorado Springs, Colorado, June 2010 – Present

Cohort Chair to monitor candidate’s research and writing activities as a cohort moves though the Computer Science Doctoral degree program. Coordinates with candidate’s mentors and readers for required deliverables. Developed the course for Foundations of Digital Security

Doctorate Level Classes Taught
Bachelor of Science in Cybersecurity Program Proposal

- Research and Writing IV (Spring 2011, Summer 2011, Fall 2011, Winter 2012, Spring 2012)
- Research and Writing III (Fall 2013, Winter 2014)
- Research and Writing VII - Research and Writing XII (Summer 2013, Fall 2013, Winter 2014)

EXPERIENCE


Systems analyst/Systems Engineer/architect providing support to Verizon Security Solutions Group. Responsible for requirement assessment, analysis and management of enterprise security product development. Responsible for translating business requirements into systems design models, designing new system applications to meet requirements, and working with enterprise architecture to ensure proposed designs meet goals of the business. Applying best practices security methods to designs and proposed architecture. Development of detailed project plans and management of change control process and Identification of project issues and develop/managed action plans to resolve issues. Communication coordination between product marketing and development teams. Provide project management as need to support assigned projects.

Network Security Specialist, Directorate of Information Management,

Fort Carson, Colorado, Feb 02 to Oct 06

Network Security Manager for the U.S. Army enclave at Fort Carson. Directly responsible for the security posture of Fort Carson’s enterprise. Intrusion detection system principal architect and analyst. Primary enforcer of security policies, processes, and procedures. Information Assurance Officer for the U.S. Army enclave at Fort Carson. Directly responsible for Fort Carson’s Information Assurance Vulnerability Alert (IAVA) program, including vulnerability scanning policies and the program’s compliance with U.S. Army
Computer Emergency Response Team requirements. Accrediting Agent for the U.S. Army enclave at Fort Carson. Developed and maintained the accreditation databases for servers, workstations, administrators, and user training. Directly responsible for managing the Regional Army Computer Emergency Response Team (RCERT) security incident reporting program and implementing corrective actions.

**Noncommissioned Officer in Charge, Battalion Intelligence Section, 1st Battalion, 68th Armor, Fort Carson, Colorado, Sep 01 to Feb 02**

Principal enlisted advisor to the Intelligence Officer regarding security. Directly responsible for the directorate’s Security Awareness, Training, and Education program. Directly responsible for the directorate’s classified and unclassified automated information systems.

**Operations Sergeant Major, Battalion Operations, 1st Battalion, 68th Armor, Fort Carson, Colorado, Oct 00 to Sep 01**

Principal enlisted advisor to the Operations Officer regarding personnel. Directly responsible for tactical deployment of the Battalion Tactical Operations Center. Recognized for keen abilities to analyze complex systems, assess both individual and organizational needs, develop and implement multi-dimensional evaluation tools. Superior ability to distinguish and organize competing priorities, while under pressure. Directly responsible for the directorate’s classified and unclassified automated information systems.

**PROFESSIONAL MEMBERSHIPS**

- Information Systems Security Association (ISSA)
- Institute of Electrical and Electronics Engineers (IEEE)
- Association for Computing Machinery (ACM)
<table>
<thead>
<tr>
<th>PROFESSIONAL DEVELOPMENT</th>
<th>Penetration Testing with BackTrack – Offensive Security, Dec 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTIVITIES</td>
<td>Tenable Nessus Vulnerability and Compliance Auditing, Nov 2013</td>
</tr>
</tbody>
</table>
Troy Jordan
Information Security : Protect, Detect and Respond

Profile


Key Skills

<table>
<thead>
<tr>
<th>Processes &amp; Foundation</th>
<th>Technologies</th>
<th>OS</th>
<th>Applications</th>
<th>Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion analysis, Incident response, TCP/IP</td>
<td>Snort, Scapy, Scada Tcpdump, nmap</td>
<td>Windows/AD Linux/Unix</td>
<td>PHP, Python, XML, SQL</td>
<td>PCI-DSS, DMCA ISO 27001/2, CSC 20</td>
</tr>
</tbody>
</table>

Education

<table>
<thead>
<tr>
<th>Year</th>
<th>Degree</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-2014</td>
<td>Masters in Computer Science</td>
<td>University of Maine, Orono (2014 expected)</td>
</tr>
<tr>
<td>1985-1989</td>
<td>Bachelor in Computer Science</td>
<td>Tufts University, Medford, MA</td>
</tr>
</tbody>
</table>

Work Experience

Information Security Lead
University of Maine System (Portland, Maine)
- Incident Handling, Intrusion Detection, Network Forensics
- DMCA Agent for UMS
- Technical lead on PCI compliance (2011-current)

Communications Specialist (LAN, WAN, InfoSec)
University of Maine System (Orono, Maine)
- Support for LAN/WAN technologies for state wide, multi-campus University
- Project lead to develop Web based Switch Management application (2004)
- Deployed first IDS monitoring (2005)
- DMCA Agent for UMS
- Technical lead on PCI compliance project (2010-2011)
- UMS Technical Representative to REN-ISAC (2009-2011)
### Instructor

**Part-time**

**Lodestone IT Workforce Training (University of Southern Maine)**
- Fall 2010
  - Authored and taught Introduction to Information Security course

### Systems and Network Administrator (Unix, Windows, GIS)

**Full-time**

**National Center for Geographic Information and Analysis (Orono, Maine)**
- 1992 to 2001
  - Maintained Unix, Windows, and Mac systems at NCGIA for all departmental functions
  - Maintained TCP/IP network infrastructure (dns, dhcp, sendmail, nis/yp, nfs, lpd)
  - Co-taught Introduction to Unix Course in SIE Department at UMaine (1994)
  - Introduced first web server to UMaine campus (1995)
  - Wrote Successful $20K grant for spatial data archive (1996)
  - Co-authored and presented academic papers at international conferences (1998, 2000)

### Research Programmer

**Part-time**

**Center for Coordination Science, Sloan School / MIT (Cambridge, MA)**
- July 1990 to Aug 1991
  - Developed new components of groupware tools for business users.
  - Successfully co-authored book chapter and conference articles on research results.

### Professional Certifications and Activities

<table>
<thead>
<tr>
<th>Certification</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>GCIA</td>
<td>GIAC Intrusion Analyst (Analyst #6658, expires 2014-07-31)</td>
</tr>
<tr>
<td>GCIH</td>
<td>GIAC Incident Handler (Analyst #7504, expires 2016-01-31)</td>
</tr>
<tr>
<td>20 CSC</td>
<td>Working Group for Assessing 20 Critical Security Controls (Council on Cyber Security)</td>
</tr>
<tr>
<td>VG’14</td>
<td>Vigilant Guard 14 – National Guard Emergency Response Exercise</td>
</tr>
<tr>
<td>USCC 2011-14</td>
<td>Instructor at US Cyber Challenge Cyber Camp (Summers)</td>
</tr>
</tbody>
</table>
Mr. Largay is an experienced technology executive with extensive leadership experience in multiple industries. He has excelled in leadership, strategy, business development, sales, technical operations, innovation and solution development with demonstrated business and technical successes. He uses his technical and business skills to deliver high value solutions to clients. He has excelled in delivering advanced and emerging technologies as an operations executive as well as “hands on” technology innovator.

Currently he is a Technology Consultant, Senior Research Fellow and Adjunct Professor at the University of Maine. His focus is Information Assurance and Cyber Security. He is founding Board Member of the University’s Cyber Security Cluster (MCSC), a leader in the creation of the Information Assurance and Cyber Security Center of Excellence focusing on Continuity of Operations and Continuity of Government, the development of the core program, its accreditation and funding. He serves as a key interface with Congress, Federal Agencies (DoD, DHS and the Intelligence Community) and Industry.

**Specialties**

- Innovation, Vision and Strategy
- Complex Solution Development Sales and Delivery
- Cybersecurity Strategy and Research (Cloud, Big Data and Threat Mitigation)
- Healthcare Solutions (HIPAA, SOX, ICD 10, COOP)
- Continuity of Operations and Continuity of Government
- Crisis Management and Disaster Recovery
- Computer and Network Forensics, Social Engineering and “White Hat”
- Compliance and Audit (NIST, GLBA, SOX, FISMA, FedRAMP)

Mr. Largay has been a principal in several startup businesses, transforming idled facilities (2005 Base Re-Alignment and Closure) for their best and highest value use, including building a High Performance Private Cloud Data Center, and composites manufacturing facility for special applications to support defense related programs.

Mr. Largay worked at the IBM Corporation as a Global Solution Executive for Global Technology Services, Global Defense and IBM Global Services. He was respected leader and innovator in those positions. He worked on IBM’s Olympic Programs, IBM’s internal Transformation Initiatives and Corporate Philanthropy efforts. He is skilled in the development and implementation of high value real world business solutions.
Mr. Largay has been a thought leader, applying commercial technologies to solve business problems and meet challenging requirements and throughout his career. He has a depth of understanding of real world business environments. He is known and sought for his insight in the application of emerging technologies, their risks and rewards, to support effective results; in short he is focused on innovation that matters.

Mr. Largay has consistently demonstrated the ability to identify and motivate teams to support real world customer requirements, where performance, compliance and cost are critical for success. He is performance driven, believes in leveraging assets and validated processes, and has delivered projects on time or ahead of schedule and when a project is troubled or delayed he rapidly identifies alternatives or mitigation strategies.

Mr. Largay’s has held many leadership positions over the past three decades in in Naval Shipbuilding, Satellite Communications, Business Continuity and Recovery, Healthcare Information Systems, Logistics, Simulation and Training, Signals and Analytics, Hardware and Software Development, Systems Integration and Testing, Network Operations and Complex Systems Architectures. He has led teams in the field in challenging circumstances. He has led the development of complex systems and their deployment for a wide range of business operations in challenging environments to support of government, commercial and other customers. He has worked effectively in the US, Europe (East and West), the Middle East and Asia.

Positions

**Yankee Logic LLC, Portland, ME – January 2007 to Present**
Managing Director of small consulting organization providing consulting services to support strategy, planning, architecture reviews and operations support to organizations facing challenging situations. He is the team leader for "second opinion" services for system architectures reviews, penetration testing, cyber risk assessment, information assurance strategies and reviews and regulatory compliance audits.

**University of Southern Maine, Portland, ME – July 2012 to Present**
Adjunct Professor, Computer Science and Senior Research Fellow at the Institute for Information and Innovation. He is a Professor for Information Assurance, Cyber Security, Continuity of Operations and Continuity of Government and focused on the discipline University wide. He is a board member of Maine Cyber Security Cluster (MCSC), and leader in its accreditation efforts as a Center of Excellence, development of partnerships with Educational Institutions, Industry and Government Agencies.

**SBA Regulatory Fairness Board Member, Region 1, ME – 2001 to Present** Mr. Largay was nominated and confirmed by the senate to serve as Maine’s representative to the Ombudsman’s Advisory Board, to deal with regulatory and compliance issues small businesses cannot resolve through normal channels. He is an advisor to the National Ombudsman, holding regional meetings on regulatory matters.
Tier-V Corporation, Brunswick, ME – 2009 to 2012
Mr. Largay served as company Director and Strategist in research and development of security and
continuity solutions. He designed and led the development of cost saving high performance deployable
composite technology solutions for customers in the defense industry.

Resilient Communications Corporation, Brunswick Maine – 2007 to 2011
Mr. Largay was a company founder and investor. He provided the vision for the reuse of key assets at the
former Naval Air Station including the transformation of the former Wing Headquarters into a high security
“Cloud Services” Data Center.

IBM Corporation, Bethesda, MD – October 2005 – December 2007
IBM Global Technology Services, Senior Solution Executive in business development, solution development
and service delivery for Global Government and Commercial clients and organizations. The offerings created
by his team were significant additions to the world class Business Continuity and Recovery Services delivered
by IBM.

IBM Corporation, Bethesda, MD – September 2001 – October 2005
IBM Global Services, Client Solutions Executive for Public Sector, Defense and Intelligence customers in the
United States and Worldwide where he demonstrated a depth of understanding of their unique and exacting
requirements for operations in a complex global network environment.

Other Positions and Assignments, 1978 – 2000

• IBM/Lotus - Senior Manager Healthcare/Supply Chain, 1997 to 2000
• IBM/ACOG – Atlanta Olympic Games, 1995 to 1997
• IBM/ISSC UK - Executive Architect Healthcare Services, 1991 to 1995
• IBM/FSD – Systems Engineer/Project Manager, 1987 to 1991
• ST Research – Systems Engineer, 1982 to 1987
• Hughes RSNE – Project Manager, 1980 to 1982
• Bath Iron Works – Technical Manager ILS, 1978 to 1979

Mr. Largay earned his undergraduate degree in Government and Legal Studies, and Physics at Bowdoin
College in 1978. He studied Electrical Engineering at the University of Maine.

He is a life member of the Armed Forces Communications and Electronics Association (AFCEA) and the
United States Air Force Association (AFA). He has continued his education at institutions around the
world, and availed himself of every opportunity to add managerial and technology training to his
“toolbox”, to refine his skills and to remain current in the rapidly changing technology landscape and the
application of new technologies and services to current business challenges.
Mark H. Rosenbaum
400 Sunset Drive • Miami, Florida 33143-6339
305-666-0505 (office) • 305-666-7000 (fax)
mhrose8989@bellsouth.net

EDUCATION
2006 – Nova Southeastern University..................................Fort Lauderdale, FL
Ph.D., 2015
Doctorate in Information System Sciences
Specialization: Computer Ethics, Privacy, Security, Policy
GPA: 3.80

2008 – 2010 Nova Southeastern University.........................Fort Lauderdale, FL
Graduate Certification in Information Systems Security
NSA and CNSS accredited program
Specialization: Computer Ethics, Privacy, Security, Policy
GPA: 4.00

M.S. in Management in Information Systems
GPA: 3.53

1987 – 1988 University of South Florida...............................Tampa, FL
B.A. Psychology
GPA: 3.72

1981 – 1987 Miami Dade Community College.........................Miami, FL
A.A.

RESEARCH and/or TEACHING INTERESTS
☐ IS/IT Security & Privacy, including Networking & Social Issues
☐ IS/IT Information Assurance & Security
☐ IS/IT Computer Ethics & Professional Responsibilities

☐ IS/IT Social & Legal Issues, Impacts, & Implications
☐ IS/IT Policies & Procedures (Security & other SOPs)
☐ Networking Technologies (General & Specific)

☐ Operating Systems (client/server) + OS Security
☐ CompTIA Courses
REFFERED JOURNAL PUBLICATIONS


PRESENTATIONS
2011 May Computer Ethics, Philosophical Enquiry Conference..........Milwaukee, WI
*IS/IT Practitioners: Privacy Violations Committed to Personally Identifiable Information.*

2010 Sept. Florida Business Women’s Association.................Fort Lauderdale, FL

AWARDS
2010 – 2011 International Society for Ethics and Information Technology (INSEIT) Fellowship: Awarded to doctoral students to facilitate collaboration and collegiality among ethics scholars (broadly defined), and increase interest in INSEIT and further its mission to promote scholarship in the field of information and computer ethics.

2010 – 2011 Osiason Educational Foundation Grant for unique dissertations in IS/IT security, privacy, and ethics

2008 – 2009 American Business Women’s Assoc. Award of Excellence for Technology Contributions

HONORS & PROFESSIONAL AFFILIATIONS
- National Honors Society IEEE – Upsilon Pi Epsilon
- Golden Key International Honors Society
- Member of the Institute of Electrical and Electronics Engineers
- Member of the Association of Computing Machinery
CERTIFICATIONS

- SLOAN-C Certification for Online Teaching
- Working on CISSP Credentials & Certifications
- CompTIA A+
- CompTIA N+

PROFESSIONAL CONFERENCES

- 2011 International Society for Ethics & Information Technology Conference (Milwaukee, WI)
- 2008 IEEE Symposium on Security & Privacy (Oakland, CA)
- 2008 Symposium On Usable Security and Privacy (Pittsburg, PA)

TEACHING EXPERIENCE

2013 Spring University of Maine – Online Adjunct Professor
- COS-375 Managing Risk in Information Systems
- COS-338 Introduction to Networking
- COS-440 Cyber-Defense/Cyber-Security

2012 Fall University of Maine – Online Adjunct Professor
- COS-340 Computer Ethics
- COS-374 Operating Systems Security

2012 Spring University of Maine – Online Adjunct Professor
- COS-338 Introduction to Networking
- COS-440 Cyber-Defense/Cyber-Security

2011 Fall University of Maine – Online Adjunct Professor
- COS-374 Operating Systems Security

2008 – 2010 Nova Southeastern University – Course Development for:
- MMIS-685 Information Security Policy, Privacy and Ethics

2009 – 2010 Nova Southeastern University – Course Development for:
- MMIS-686 Information System Auditing and Secure Operations

2009 – 2010 Macon State College – Course Development for:
- ITEC-2201 Business Information Applications & Computer Technology
Work Experience

University of Maine at Fort Kent 2011 – Present
Online Adjunct Professor
Dedicated doctoral candidate with demonstrated success in online classroom education within the disciplines of IS/IT and MIS curriculum – responsible for teaching, student advising, and departmental program development to meet with national accreditation with National Security Agency and Department of Homeland Security standards. Blackboard development.
- Architect Security and Information Assurance Program to Meet NSA/DHS accreditation
- New and Existing Curriculum Development
- Teach Courses
- Technical Training
- Advise and Mentor Students

Kompute LLC. 2002 – Present
Independent IS/IT Consultant/Contractor Miami, FL
Perform and direct multifaceted tasks related to IS/IT environments for businesses with 5-100 employees with budgeting up to $200k. Professional technology services of strategic management, vendor liaisons, and tactical planning. Define and execute IS/IT strategies using ROI, CBA, TVA, SecSDLC, and other capacity planning tools. Perform technology implementation and training. Recommend and implement IS/IT networking best practices and procedures for secured and non-secured wired and wireless environments. Also provide systems analysis, development, and design.
- Technical Training
- Network design, implementation, & performance monitoring
- Baselining, needs analysis, capacity & resource planning
- Mid-size to small-scale consolidation of network resources
- Development SOPs & other issue specific IS/IT documentation
- Network security / Security & privacy policies
- NIST 800 Security Model framework compliance
- Disaster resource planning
- Web filtering & monitoring
- Systems hardware and application training
- Develop multiple types of survey questionnaires related to products of IT/IS operations and user satisfaction
- SETA – Security Ethics Training and Awareness
Global Precision Inc. 2003 – 2004
Sr. Network Systems Admin/Engineer Davie, FL
Responsible for the daily operations of the corporation’s internal servers, PC’s and peripherals, as well as any and all initial planning, development and maintenance of all system hardware and software for Windows, Linux and Unix systems.
- Completely designed and implemented Web filtering systems
- Responsible for PIX & Checkpoint firewalls, plus various routers, switches, etc. & diagnostics of known system issues & network management
- Wrote privacy and security policies
- Redesigned and implemented network security
- Responsible for daily corporate data backups
- Charged with the responsibility of cultivating and maintaining liaisons with all distributors and individual corporate vendors for IS/IT purposes
- Took charge of all IS/IT inventory management
- Conducted all end-user training for network security and software needs
- Developed the company’s working set of network SOP’s including network security
- Implemented weekly network status reports
- Lead capacity planning team
- Maintained project timelines
- Technical Training

Fabulous Finds/Fabulous Baskets 2001 – 2003
Part time MIS Manager Miami, FL
Set company’s IS/IT goals and objectives. Coordinated IS/IT activities of company which included but was not limited to, needs analysis for training, hardware and software upgrades. Responsible for weekly business reports to company owner.
- Built, installed, configured, upgraded PC’s and networks
- Troubleshoot networks issues
- Coordinate activities of budgeting issues for IS/IT projects
- Wrote all IS/IT SOP’s including disaster recovery and network security
- Technical Training

Nuclear Regulatory Commission 1996 – 1996
Asst. Network Operations & Project Mgr. Rockville, MD
Contract position with Sytel, Inc.
- Administered and performed strategic day-to-day operations of MIS division and technology services for network assistance operations center
- Managed the technical team of 25 technicians, engineers, helpdesk operators
- Responsible for trend analysis and monthly reports of 1000+ helpdesk calls
- Liaison between NRC and contractors office for project mgt. issues
- Identify & re-engineer trouble areas for process flows within operations
- Conduct weekly staff and operations meetings
- Forecast budgeting & equipment needs
- Responsibility of hiring new technical staff hires as well as their training
- Provide weekly status reports on all operations issues
- Managed and coordinated all resources to ensure proper staffing during core hours of operations.
- Performed hardware/software installs for system configurations of testing COTS evaluation in Windows and UNIX environments
- Responsible for various project management implementations, as well as ROI, CBA, and TVA assessments
- Technical Training
- Conducted test phases of new systems architectures

**JLP Networking Company. 1994 - 1996**  
*Dir. of Network & Project Mgt. Services* Fairfax, VA

**Computer Networking Company. 1991 - 1994**  
*Dir. of Network Services – Project Mgt.* Fairfax, VA

**Gold Coast Computing 1989 – 1991**  
*Asst. Tech Mgr.* Tampa, FL

**Mega Byte Computer 1986 – 1991**  
*Consultant* Tampa, FL

**The Godfather BBS 1986 – 1989**  
*Asst. Sys. Admin.* Tampa, FL
Edward Sihler

(a) Professional Preparation

- University of Virginia: International Relations, B.A. 1990
- University of Iowa: Computer Science, B.A. 2000
- University of Iowa: Computer Science, MCS 2005

(b) Professional Appointments

2012 - Technical Director Maine Cyber Security Cluster, University of Maine
2012 - Scientific Systems Administrator, Institute for Information and Innovation, University of Southern Maine, Portland, ME
2011 – 2012 Systems Specialist, Information Services, Maine Medical Center, Portland, ME
2006 - 2010 Systems Programmer, Department of Orthopedic Surgery, University of Michigan, Ann Arbor, MI
2000 - 2005 Teaching Assistant, Department of Computer Science, University of Iowa, Iowa City, IA
1998 - 1999 Systems Analyst, Iowa College of Medicine, University of Iowa, Iowa City, IA
1994 – 1998 Senior Network Engineer, Information Services, Wake Forest School of Medicine, Winston-Salem, NC
1993 – 1994 Desktop Support, Information Services, Northern Telecom, RTP, NC

(c) Products


(d) Synergistic Activities

ISO / IEEE work: Editor for Section 5 of ISO / IEEE standard P23026 working group

(e) Collaborators & Other Affiliations
Collaborators and Co-Editors:

Chester Chan, Dr. Richard Hughes, Dr. Bruce Miller MD, The University of Michigan
Dr. Ghazi Alkhatib, Princess Sumaya University
Ayanda Dauda, University of Ibadan
Diwakar Gan, (Ret.)
Dr. Wayne O’Brien, Ratheon
Dr. Kalum P. Udagepola, KU Geomatic Pty Ltd.

Graduate Advisors and Post-Doctoral Sponsors:

Dr. Sukumar Ghosh, the University of Iowa

Thesis Advisor and Postgraduate-Scholar Sponsor:

Dr. Douglas W. Jones, the University of Iowa
(a) Professional Preparation
University of North Carolina at Greensboro, English/Philosophy: B.A., 1974
Appalachian State University, Instructional Media: M.A. 1980

(b) Appointments
2012- Present, Director, Maine Cyber Security Cluster

2005- Present Director, Information and Innovation, Research Initiatives and
Associate Research Professor, Department of Technology,
University of Southern Maine, Portland Maine

2001 – 2005 Senior Scientist, Institute for Research in Information Science
Associate Research Professor Department of Technology,
University of Southern Maine, Portland Maine

1997 – 2001 Computer Projects Coordinator, Electrical Engineering Department, University of
Southern Maine, Portland Maine

1993 – 1997 Assistant Professor, Instructional Media, Appalachian State University, Boone, North
Carolina

1990 – 1992 Co-Director IU/IBM Multimedia Project, Indiana University, Bloomington, Indiana 1987
- 1989 Campus Liaison for Technological Services, Indiana University System, Bloomington,
Indiana

(c) Products
Co-Chair Steering Committee, with Mr. George Hogan, CIO, Wright Express, of State-Wide CS_IT
Initiative – Project Login - commissioned by former Chancellor Dr. Richard Pattenaude and with
current Chancellor Dr. James Page, UMS, and Mr. Mike Dubyak, CEO Wright Express. Worked
with CEO’s, CIO’s, owners, from major business and industry partners, and faculty from all UMS campuses. Oversaw the development of the CS_IT campaign and the development of the recommendations for implementing the program for doubling the number of CS and IT graduates from the UMS over the next four years. (2011 to present).

(d) Synergistic Activities

PI, Maine Cyber Security Cluster, Maine Technology Institute (CIP 146) Awarded Summer 2012, working with business and industry, state government and university faculty, staff, and expert practitioners to create a cluster for cyber security in Maine.

Co-PI Acquisition of Integrated Electron Microscopy, Tomography and Computational Resources Supporting Interdisciplinary Collaboration in Research and Education at USM, NSF 0521262, Award July, 2005

Primary Technical Consultant for National Science Foundation, HRD-0099141, Earth System Science Ideabook. Provided comprehensive technical support on graphic design, web development, programming, hosting, and overall web-based communication for ESSIB. http://research.usm.maine.edu/earth

Director of Information and Innovation at USM working with researchers in the areas of Physics, Chemistry, Statistics, Environmental Science, Computer Science, Technology, Biology, Aquatic Systems, Public Health, Nursing, Cyber Security, and Art to create http://research.usm.maine.edu

(e) Collaborators and Other Affiliations

Collaborators:
Dr. Clare Bates Congdon, Computer Science, University of Southern Maine
Dr. Monroe Duboise, Applied Medical Science, University of Southern Maine
Dr. Samantha Langley-Turnbaugh, Environmental Science University of Southern Maine
Dr. Bruce MacLeod, Computer Science, University of Southern Maine
Dr. Bruce Segee, Computer Engineering, University of Maine
Mr. James R. Smith, CIO State of Maine
Mr. Richard Thompson, CIO University of Maine System
Mr. Mike Dubyak, Wright Express (WEX)
Mr. Don Kennel, IDEXX
Ms. Andrea Roma, UNUM

Graduate and Post Doctoral Sponsors
Graduate Advisors: Dr. Thomas Schwen, Emeritus (Indiana University), Dr. Myrtle Scott, Emertia (Indiana University), Dr. Dennis Pett, Deceased (Indiana University)

Thesis Advisor and Postgraduate-Scholar Sponsor
Graduate Advisee: Margaret Chen, Ed.D Appalachian State University, 1997
External Reviewers’ Reports
Executive Summary

I have completed my review of the materials provided in support of the proposed Bachelor of Science in Cybersecurity Program. In general I find the program to be promising, built upon strong, established coursework, already demonstrating outstanding external recognition and to be offered by well qualified faculty. It is my opinion the program, as described, is worthy of approval and implementation. It will be successful and popular.

The establishment of the degree program as the cornerstone of the widely respected Department of Homeland Security/National Security Agency (DHS/NSA) National Centers of Academic Excellence in Information Assurance/Cyber Defense program is a strong proponent for its design. With the radical improvement in the specifications for coursework mapping to general Cyber Defense criteria, and the optional mapping to specific Focus Areas, the recognition of a program as part of this program speaks volumes as to its breadth, depth and appropriateness to the discipline. The further association with the NICE framework, which currently is parallel but not integral to the DHS/NSA course mapping, also increases the expectation of quality and suitability of the program.

It is both the strength and weakness of courses offered at traditional liberal arts universities like ours, that so much of the students’ educational time is devoted to non-major specific content. While some private schools are able to offer security programs without the general education requirements found in most public university, and as described in the program proposal, I find that in this instance the specific foundation described will strongly support the students matriculating from this degree program.

The list of faculty provided indicate strong support for the capability of the partnered institutions to provide the described program. Both the research and instructional credentials of the faculty listed, as evidenced in their attached vitae, provides assurance that, workload permitting, the consortium should have no issues providing the expertise needed to conduct the degree program. I find the provided enrollment figures to be very reasonable to the point of being overly conservative. I expect the program will become popular rapidly, and the faculty should make plans to expand the program rapidly should demand rise. As the proscribed purpose of the degree is to create cybersecurity professionals, in general, I find the quality of the proposed program to be very good.

The proposal does well in making the same arguments we in academic, industry and the government section have been attempting to make for years. There just aren’t enough qualified information security professionals available considering the scope of the problem at hand. As the “attackers” move from individual miscreants to professional crime organizations, the need for talented individuals who can assess and remediate risk to the level an organization can accept grows.
exponentially each year. We just cannot create enough graduates in this demanding field, especially considering the field itself is still in its infancy, and poorly understood by the general populace.

**Foundation**

In reviewing an academic program, one must always begin with the end goals or objectives of the program. Upon completion of this program, where will the graduates be qualified to work? At what level? With what fundamental skill sets? What are their career progression goals and objectives? At Kennesaw State our graduates are focused on working in mainstream business, in virtually any industry, beginning with entry positions at a Helpdesk, Information Security department as a security systems administrator, or as a low-level security manager responsible for policy, risk management and/or regulatory compliance. Their career goals lead them toward positions as Chief Information Security Officers (CISOs) at any one of the tens of thousands of businesses operating globally. We focus on fundamental, business-oriented graduates capable of designing, implementing and administering security solutions using current technology.

A study of information security positions, done by Schwartz, Erwin, Weafer, and Briney, found that the information security positions can be classified into one of three areas: Those that define information security programs, those that build the systems and create the programs to implement the information security controls within the defined programs, and those that administer the information security control systems and programs that have been created. Definers provide the policies, guidelines and standards…They’re the people who do the consulting and the risk assessment, who develop the product and technical architectures. These are senior people with a lot of broad knowledge, but often not a lot of depth… [Builders are] the real techies, who create and install security solutions… [Administrators] operate and administrate the security tools [and] the security monitoring function and…continuously improve the processes, performing all the day-to-day…work…We often try to use the same people for all of these roles. We use builders all the time… If you break your InfoSec professionals into these three groups, you can recruit them more efficiently, with the policy people being the more senior people, the builders being more technical and the operating people being those you can train to do a specific task. [Cite available on request]

This cite has become the cornerstone of our understanding of academic programs in information security, as we are able to determine at a very general level what it is that the program seeks to instill in its students and promote in its graduates. My institution produces Administrators that aspire to be Definers. With this foundation in mind, I begin with my assessment of the proposed program.

**Overview**

The Proposed BS-Cybersecurity is built upon existing courses at multiple institutions. It purports to be able to roll out the new degree program with little extra support in terms of resources. The materials presented support this assertion, as the curriculum is, for the most part, already established, and well defined.

While it has become quite mainstream, I always hesitate at titles of programs that seek to capture the current industry “fad” terminology. Cybersecurity was originally defined as the
 protección de información mientras se encuentra en red, como su origen el término “cyberspace”. No obstante, con la adopción del término por el gobierno federal, no estoy completamente en contra de su uso en el título de un programa, pero con cautela promoviendo el programa como se interpretará como enfocado prácticamente exclusivamente en la información de Internet, cuando el papel del verdadero profesional de seguridad de la información es proteger la información de cualquier tipo, en cualquier parte, en todo momento.

La reconocimiento del currículum como el componente de mapeo del DHS/NSA CAE IA/CD reconocimiento es anticipado y un punto fuerte del currículum. Recientemente hemos reconocido nuestros programas y la institución bajo este programa, el que sólo ha existido durante un año. De la misma manera, la asociación a siete instituciones significa que no se necesitarán todos los recursos necesarios para el programa. Proporcionará no habrá impedimentos para la matriculación física de los estudiantes, siendo otro punto fuerte que vale la pena destacar.

Como un lado, no estoy seguro de lo que significa por “entrega de servicios de seguridad informativa basada en computadora”. ¿Estás refiriendo a terceros servicios de seguridad? ¿Hay tal presencia de tales organizaciones en la economía local que elige empleados de nivel de entrada de tal cantidad para justificar el grado? Me temo que esta declaración generará más preguntas que resuelve.

Como los revisores de esta propuesta sin duda no serán expertos en Cybersecurity, sugiero definirlo temprano, en el Programa Descripción/Objetivos sección o mucho antes. En su lugar, declaraciones como “el Bachelor de Ciencia en Cybersecurity se ha diseñado para preparar a los estudiantes para obtener empleo en el campo de la Cybersecurity o como estudio de graduado en Cybersecurity” se vuelven difíciles de interpretar. Me gustaría también recomendar la modificación de la declaración para incluir “o áreas relacionadas” en el componente de estudios de graduado. Según mi experiencia, la mayoría de empleadores prefieren sus empleados tener diferentes pero relacionados grados de pregrado y graduados, especialmente dada la lista de grados de pregrado que adelante, no incluyen un grado de pregrado específicamente en Cybersecurity.

No creo que te necesites promover una diferenciación entre Cybersecurity y Information Assurance como temas. IA y Cybersecurity se pueden argumentar razonablemente como el mismo tema, y superponen significativamente con la Información Seguridad. En mi experiencia, IA es el término usado por el gobierno federal, que recientemente ha sido reemplazado por Cybersecurity. La Información segura es el término que se ha utilizado por la industria desde el cambio de Information Systems Security o Information Technology Security en la década de 90’.

Educational Quality

El establecimiento de la program como el eslabón central del ampliamente respetado DHS/NSA CAE programa es una propuesta fuerte para su diseño. Con la radical mejora en las especificaciones para el mapeo de los estudios a la Defensa Cibernética, y la opción de mapeo a específicas Focus Areas, la reconocimiento de un programa como parte de este programa habla volúmenes en cuanto a su amplitud, profundidad y apropiación a la disciplina. La asociación adicional con el NICE framework, que, desafortunadamente, actualmente es paralelo pero no integral a la DHS/NSA mapeo, también aumenta la expectativa de calidad y sostenibilidad del programa.
Regarding projected enrollments, I find the provided figures to be very reasonable to the point of being overly conservative. I expect the program will become popular rapidly, and the faculty should make plans to expand the program rapidly should demand rise.

I define quality as “fitness for the proscribed purpose”. Thus, as the proscribed purpose of the degree is to create cybersecurity professionals, in general, I find the quality of the proposed program to be very good.

**Specific Comments in Educational Quality**

In your Section D. Accountability, pg. 9, you assert your program is unique. I would, however like to hear how, beyond the statements provided, as all institutions with new degree programs “focus on optimized use and existing resources” and many programs I have seen “use collaborative-based synergy”. Find something that makes your program truly unique and flaunt it.

I stress caution in any higher education degree program that claims to prepare students for “optional professional certification (e.g. CompTIA Security+)”. In my experience, the higher education degree in the field is far superior to these entry level certifications. In fact, the content of the entire Security + is far less than the knowledge provided in most introductory information security courses. For those with a general Associate’s degree, yes the CompTIA certificates provide additional credentials, but for those with a Bachelor’s degree, such entry-level certifications are superfluous. However, advanced certifications (GIAC for technical, CISSP/CISM for managerial focus) would provide additional credentials, however, the majority of these require experiential components, and thus are designed for professionals with at least a few years on the job.

I also stress caution in a proposal designed to “raise awareness and interest of students in …” other Bachelor degree programs. It is quite logical to promote follow-on graduate coursework, but to indicate in your proposal you intent to influence students to obtain a different degree program seems counter-productive. Perhaps rewording this to indicate that dual degrees are promoted, along with follow-on graduate work, would improve the suitability of this section.

**Appropriateness of Curriculum**

The core of any effective degree program is its curriculum. At face value, the content appears suitable for a general computer science/computer security hybrid degree program. As the material provided did not include the course syllabi for existing courses or the proposals for any new courses, which were also not readily discoverable on the web, I am unable to comment in detail about the suitability of particular courses.

It is both the strength and weakness of courses offered at traditional liberal arts universities like ours, that so much of the students’ educational time is devoted to non-major specific content. While some private schools are able to offer security programs without the general education requirements found in most public university, and as described in the program proposal, I find that in this instance the specific foundation described will strongly support the students matriculating from this degree program. If there were any space available in the major or general electives I would encourage the developers of the program to emphasize business courses as a minor or elective option.
If I am to presume that the courses listed are typical of course of the same titles at our, and neighboring, programs then I feel the curriculum is very suitable to the proposed purpose of the degree program. The list does not expound on the approved DHS/NSA IA Focus Areas, nor are they described elsewhere in the document. It is rather unusual to find these topics in a CS oriented security program, providing what I feel is a much needed balance to an otherwise technology heavy degree program.

In general, a degree program of this type, which relies on a CS foundation must expect that the existing CS courses will undergo some level of transformation to convert traditional programming and software engineering courses into Software Assurance courses, teaching secure development from day 1, rather than attempting to “bolt on” additional security courses after Programming Principles have been instructed. Your learning outcomes specifically call out “employing an approved secure systems development process model” but without descriptions and details I am unable to comment on how well implemented that goal is.

As an aside, in the list provided you have two CYB 370 courses – one is OS Security, the other Policy, Law, Compliance, Ethics – II.

**Structure of Program**

As the proposal purports the new degree program to Online (Hybrid), I would expect that the degree will have distinct challenges in teaching many of these courses online. It was not until we deployed an extensive cloud-based Virtual Machine sandbox (NetLab+ appliance and supporting ESXi servers) were we able to offer our similar courses completely online. I would have liked to have read more about how the proposed degree program plans to deal with the challenges of offering hands-on computer labs online, or in a hybrid format even.

**Quality of Faculty**

The list of faculty provided indicate strong support for the capability of the partnered institutions to provide the described program. Both the research and instructional credentials of the faculty listed, as evidenced in their attached vitae, provides assurance that, workload permitting, the consortium should have no issues providing the expertise needed to conduct the degree program. Meeting a rising demand once the program gains popularity is another issue, which will need to be addressed once the program is implemented.

**Summary Comments**

Having reviewed the entire proposal, I still find myself drawn back to my opening comments. What do you want your graduates to do? What fields, industries, and organizations will they work in? I get the general sense that, using my Schwartz, et al. definitions, you want to create Builders, who can “produce effective designs and solutions for specific cybersecurity problems”. In my opinion, that’s the only major-specific learning outcome, and it’s a bit ambiguous. The rest are general technology and/or college outcomes, and in one case relatively immaterial to an undergraduate degree program (the “scholarly and professional literature” #2, pg. 9). Your number 7
goal, “Use appropriate tools to detect an attack and determine appropriate remedial action based on its progress” while very specific, omits the fundamental “preventative” and “recovery” aspects of sound Incident Response methodology (Prevent, Detect, React, Recover). Since I don’t see a specific course on Incident Response and without course syllabi I am unable to determine how pervasive this subject is in the degree curriculum, I question the inclusion of this as a program objective.

The program has strength and depth in network security (from Intro to CS and InfoSec to Networking to Network Security to OS Security to Cyber Defense). Programming/scripting supports this depth. I would expect this to be the explicit selling point of your degree program, and your majors, rather than developing designs and solutions. Perhaps this is what you intended; if so, it needs to be much more explicit.

The proposal does well in making the same arguments we in academic, industry and the government section have been attempting to make for years. There just aren’t enough qualified information security professionals available considering the scope of the problem at hand. As the “attackers” move from individual miscreants to professional crime organizations, the need for talented individuals who can assess and remediate risk to the level an organization can accept grows exponentially each year. We just cannot create enough graduates in this demanding field, especially considering the field itself is still in its infancy, and poorly understood by the general populace.

In summary, I do feel the program, as described has great merit and is worthy of implementation. I hope you will accept the criticism here as an effort to assist you in creating a document that is easily recognized as proposing a program dramatically needed across the country.

I wish you the best in getting this program approved and implemented. Please contact me if you have comments about this review.

Sincerely,

Michael E. Whitman, Ph.D., CISM, CISSP
Executive Director, Center for Information Security Education
Professor of Information Security Kennesaw State University
560 Parliament Garden Way, MD 0405
Kennesaw, GA 30144
Review of the proposed Bachelor of Science in Cybersecurity Program
For the University of Maine System

Prepared by:

Dr. Doug Jacobson  
University Professor, Dept. Electrical & Computer Engineering  
Director: ISU Information Assurance Center  
Iowa State University  
Ames, Iowa.

This proposal calls for the creation of a BS in Cyber Security using existing courses and faculty from several universities with the University of Maine system. The authors of the proposal make a strong case for the development of a BS in Cyber security based on the need from potential employers.

Below are a set of comments, issues, and questions based on my review of the proposal:

Quality of the proposed degree

The degree is focused on cyber security and defense and will produce students that can work in the area of computer and network defense. The authors are aligning their degree with the NICE workforce framework. The NICE framework is in the early stages and is not widely adopted by all employers. It would be good to see input from employers maybe in the form of an advisory board. The input from employers also helps in their plans to have internships for the students.

Since the authors say no new courses are created it would have been nice to see a little more information about the security courses, especially the capstone course. Without seeing the content of the courses it is hard for me to tell the overall quality of the degree. The number of security courses seems a little light, but there may be more security content within the “non” security courses.

 Appropriateness of the curriculum

Proposal indicates a prototype curriculum and that the “Precise specification of suitable course numbers/titles amenable to a “systems-oriented” degree is under development pending formal approval.” The prototype curriculum does appear to meet the goals outlined by the proposers. Their goal to maintain mapping to the NSA/DHS CAEIA/CD curriculum Knowledge Units is a good idea.
The authors need to keep an eye on the efforts underway to create an ABET accredited set of program criteria for cyber security. This effort is in the very early stages and has no effect on current proposal. However, someone from the program should at least keep track of the ongoing efforts. This program could become one of the first ABET accredited programs.

**Structure of the program**

The proposal talks about a hands on approach to teaching cyber security. This approach is needed given the goals for the degree and the types of students they are wanting to produce. I would have liked to seen more discussion about the types and amount of labs. There also needs to be some discussion of how labs will be handled between the various campuses (remote lab access, or duplication of labs). Another concern is the number of students in the program and plan to handle the hands-on learning. The lab resources (TAs, equipment, space) can become a limiting factor on the programs growth.

It would be good to indicate which schools are offering which courses and more details on the overall structure of the partnership. It is unclear what students will be experiencing when they are at each school.

The portfolio requirement is a great idea and can help the students during their job search. We have used portfolios for over 10 years and have found them to be very useful. We discovered early on that we needed to talk with the students about the portfolios in their sophomore year so they would start collecting materials throughout their college career.

**Quality of the faculty**

The faculty are very well qualified to implement the degree. The only concern is the number of faculty members based on the projected growth of the program. I think their growth numbers are conservative and the proposal does not address the need for multiple sections of classes or the increased advising load. The proposal also does not address the extra burden of teaching a lab based curriculum in a subject area that changes so quickly. Cyber security labs require constant updating.

**Assessment of student outcomes**

The proposal outline several student outcomes which are very appropriate to the proposed degree. While the format for the proposal does not lend its self to discussion of assessment, the proposers should develop an assessment plan to measure the student outcomes based the ABET guidelines. They do mention the portfolio as one tool for assessment, this is a perfect use for the portfolios and we have even added a couple of items students must address in their portfolios to help with assessment.
Comments and questions from the proposal

I have a few general comments on various items I saw in the proposal.

1. On page 6 the authors talk about preparing students for advanced education in cyber security. It is unclear that this program will be able to do that. As I stated above this is a great proposal and the proposers will create a solid BS in cyber security, it is unclear how this would fit into many of the current graduate programs.

2. On page 6, the authors talk about preparing students for professional certificate. Depending on the type of certification this can be difficult. Some certifications can be taught as part of the courses and others are more difficult to prepare for. The proposers are unclear about which type they are trying to prepare students for.

3. On page 9 there is a short description of what is called accountability. If this is meant to be a section on program assessment then this section needs some work. Not sure if this is meant to be accountability of the student outcomes or the overall program itself.

4. The authors have talk about articulation from community colleges. I’m not familiar with the educational system in Maine. I know in my state we have issues with articulation from what is often referred to as vocational technology degrees. In Iowa many of the credits from the vocational tech degree do not transfer to many of the 4 years schools.

5. The authors should have some discussion on recruitment. I think they will have no problem getting students. I think a more complex issue to making sure they make it clear what type of students they are looking for and what they are producing. For example, the authors talk about employers in Maine, but there are students that would be looking for jobs in DC at places like NSA, DHS, FBI. I’m not sure this degree the types of students these agencies are looking for.

6. I’m not sure that the discussion on page 24 is right. !gain not knowing the enrollments of the other degrees (CS, etc.) it is hard to tell if this degree will “take” students from the other majors or the growth will be in new students.

7. Has there been any discussion about also adding a minor for students in CS. This is a general comment and is not meant to be negative.

8. Not sure this is needed or required, but is there some type of governance document that helps provide authority to the faculty across schools and departments. At my school any program that is jointly run across departments or schools has a document describing how issues are handled, how changes are made to the curriculum etc. This all might be covered in the MOU, which is still under development.

Final conclusion

This is a well thought out idea and should be approved. The need for this degree is well documented and the idea of a jointly run degree is a great idea.
Preliminary Findings of USM MBA Students’ Market Research
MARKET RESEARCH FOR MCSC

Maine Cyber Security Cluster’s resources and services span many segments of the cyber security industry, including research and development, training and education, and leasing of infrastructure. This diversification of products and capabilities allows MCSC to adapt to the constantly evolving cyber security industry.

PUBLIC SECTOR

The public and private sectors are both experiencing increased volume and sophistication of cyber security threats. As reported by CNN in 2014, “there were almost 61,000 cyber attacks and security breaches across the entire federal government last year according to a recent Obama administration report. And the number of cyber incidents involving government agencies has jumped 35 percent between 2010 and 2013, from roughly 34,000 to about 46,000, according to another recent report by the Government Accountability Office.”

Among the cyber threats included a breach of cyber security for the Army Corps of Engineers in early 2014 when hackers accessed sensitive information about 85,000 dams. The hacked data included the dams’ location, condition, and potential for fatalities if the dams were to be breached.

In addition, cyber threats have increased the strain and complexity of international relations. The New York Times reported that “Iranian hackers were identified as the source of coordinated attacks against more than 50 targets in 16 countries, many of them corporate and government entities that manage critical energy, transportation and medical services.” To combat these threats, the US has become publicly offensive in its tactics. Proactive cyber security was “critical to a yearslong American and Israeli cyberattack on Iran’s nuclear facilities, and descriptions of the placement of “implants” in foreign computer systems — for surveillance and potential offensive action — run through thousands of pages of documents released by Edward J. Snowden, the former National Security Agency contractor.”

According to the formal White House foreign policy statement, “President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter.”

BUDGET

President Obama made the United States government’s increasing focus on taking proactive measures to establish a front line of defense against today’s threats very clear in his 2016 budget proposal to allocate $14 billion to cyber security. The budget included proposals to distribute the funds across major government agencies including the Department of Homeland Security, Department of Justice, and Department of Defense including the following initiatives:

---

5 http://www.nytimes.com/2015/03/20/us/us-must-step-up-capacity-for-cyberattacks-chief-argues.html?ref=topics&_r=0
6 https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
- Department of Homeland Security requested “$480 million for programs that stop malicious attacks against government computers, and another $100 million for hardware, software and support services that provide continual support of federal networks.” 8
- The Justice Department requested an additional $27 million to its current estimated spending of $500 million to spend on cyber investigations and prosecutions in order to specifically target cyber criminals. 9
- “The FBI is asking for an additional $10 million to improve “cyber collection and analysis” and to ensure it has the capabilities it needs to investigate crimes that involve the Internet and cyberspace. That would join the FBI’s current cyber budget of about $470 million.” 10

PRIVATE SECTOR
In an official statement, the White House emphasized the breadth and scope of cyber security threats facing the US saying “Cyber threats targeting the private sector, critical infrastructure and the federal government demonstrate that no sector, network or system is immune to infiltration by those seeking to steal commercial or government secrets.” 11 The hacking of SONY Pictures Entertainment and Anthem Inc. highlights the impact a cyber security breach can have on a private sector company. An Anthem spokesperson reported that “the database that was penetrated in a previously disclosed hacker attack included personal information for 78.8 million people, including 60 million to 70 million of its own current and former customers and employees.” 12 As society becomes more reliant on technology, the infrastructure we rely on becomes more vulnerable to cyber attacks such as Corporate Security Breaches, Spear Phishing, and Social Media Fraud. 13 Internet security company, Symantec, published the following findings 14 as part of its 2014 Internet Security Threat Report showing the impact of cyber security on individuals:

- 91% increase in targeted attacks campaigns in 2013
- 62% increase in the number of breaches in 2013
- Over 552M identities were exposed via breaches in 2013
- 38% of mobile users have experienced mobile cybercrime in past 12 months
- One in 392 emails contain a phishing attacks
- Web-based attacks are up 23%
- 1 in 8 legitimate websites have a critical vulnerability

EMPLOYMENT
As seen by the prevalence of cyber security threats across the public, private, and individual levels of society, preventing and/or managing these cyber security breaches is essential to protecting

12 http://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364
13 http://www.dhs.gov/topic/cybersecurity
our economy and welfare. With the increase of threats also comes an increased demand for cyber security professionals.

To better understand the employment demographic, we can examine the Bureau of Labor Statistics for Information Security Analysts (defined as employees that “Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses.” (15-1122)\(^\text{15}\) As reported by the BLS\(^\text{16}\):

<table>
<thead>
<tr>
<th>Quick Facts: Information Security Analysts</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>2012 Median Pay</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Entry-Level Education</strong></td>
</tr>
<tr>
<td><strong>Work Experience in a Related Occupation</strong></td>
</tr>
<tr>
<td><strong>On-the-job Training</strong></td>
</tr>
<tr>
<td><strong>Number of Jobs, 2012</strong></td>
</tr>
<tr>
<td><strong>Job Outlook, 2012-22</strong></td>
</tr>
<tr>
<td><strong>Employment Change, 2012-22</strong></td>
</tr>
</tbody>
</table>

Nationally, the BLS reports a 37% change in employment between 2012 and 2022 compared to the national average of 11% across all occupations. (Chart below)\(^\text{17}\)

\(^{15}\) http://www.bls.gov/oes/current/oes151122.htm
\(^{16}\) http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
\(^{17}\) http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6
The BLS attributes this high growth to:

The federal government is expected to greatly increase its use of information security analysts to protect the nation’s critical information technology (IT) systems. In addition, as the healthcare industry expands its use of electronic medical records, ensuring patients’ privacy and protecting personal data are becoming more important. More information security analysts are likely to be needed to create the safeguards that will satisfy patients’ concerns.\(^\text{18}\)

In addition, annual wages for information security analysts range from $50,300 for the lowest paid 10% up to and above $140,460 for the highest 10%. The expected job growth as well as salary range is very favorable for students and recent college graduates looking for employment in the cybersecurity field.

\[
\begin{array}{c|c|c|c|c|c}
\text{Percentile} & \text{10\%} & \text{25\%} & \text{50\% (Median)} & \text{75\%} & \text{90\%} \\
\hline
\text{Hourly Wage} & $24.18 & $32.23 & $42.74 & $54.80 & $67.53 \\
\text{Annual Wage} & $50,300 & $67,030 & $88,890 & $113,990 & $140,460 \\
\end{array}
\]

\(^{18}\text{http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6}\)
We can further examine the prevalence of information security analysts by state to clearly see a concentration in metropolitan areas, including the East Coast, but a only 50-240 individuals in Maine.19

In order to meet the demanded increase in cyber security employees, more people must be entering the industry and acquiring the necessary cyber security skill set, usually in an academic setting. The National Initiative for Cybersecurity Careers and Studies (NICCS) created a framework that defines the responsibilities and professional requirements of cyber security workers. The “Framework” organizes the cybersecurity industry into seven specialty areas: Securely Provision, Analyze, Operate and Maintain, Oversight and Development, Collect and Operate, Protect and Defend, and Investigate.20 While there are many sub-categories within each field, these are the seven core components that NICCS defines as essential to working in the cyber security workforce. It is important that new employees to the industry are well prepared and equip to meet the changing demands of cyber security threats.

19 http://www.bls.gov/oes/current/oes151122.htm
20 http://niccs.us-cert.gov/training/tc/framework/categories
## Financial Model

### Computer Science Credit Hours

<table>
<thead>
<tr>
<th></th>
<th>Year 1 - 2016</th>
<th>Year 2 - 2017</th>
<th>Year 3 - 2018</th>
<th>Year 4 - 2019</th>
<th>Year 5 - 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong># of Students</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fall</td>
<td>15</td>
<td>28</td>
<td>41</td>
<td>57</td>
<td>69</td>
</tr>
<tr>
<td>Spr</td>
<td>12</td>
<td>23</td>
<td>35</td>
<td>49</td>
<td>60</td>
</tr>
<tr>
<td>Total # Credit Hours</td>
<td>225</td>
<td>415</td>
<td>628</td>
<td>866</td>
<td>1,061</td>
</tr>
<tr>
<td><strong>Computer Science Credit Hours</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Focus</td>
<td>45</td>
<td>111</td>
<td>192</td>
<td>255</td>
<td>312</td>
</tr>
<tr>
<td>Electives</td>
<td>49</td>
<td>111</td>
<td>192</td>
<td>255</td>
<td>312</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>94</td>
<td>219</td>
<td>382</td>
<td>477</td>
<td>624</td>
</tr>
</tbody>
</table>

### Computer Science Total Revenue (Tuition, Fees & Course Fees)

<table>
<thead>
<tr>
<th></th>
<th>Year 1 - 2016</th>
<th>Year 2 - 2017</th>
<th>Year 3 - 2018</th>
<th>Year 4 - 2019</th>
<th>Year 5 - 2020</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td>13,765</td>
<td>33,926</td>
<td>58,329</td>
<td>77,352</td>
<td>94,730</td>
</tr>
<tr>
<td><strong>Electives</strong></td>
<td>49</td>
<td>111</td>
<td>192</td>
<td>255</td>
<td>312</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>13,716</td>
<td>34,037</td>
<td>58,520</td>
<td>77,607</td>
<td>94,442</td>
</tr>
</tbody>
</table>

### Computer Science Section Counts

<table>
<thead>
<tr>
<th>Focus Courses</th>
<th>#Credits</th>
<th># of Sections</th>
<th>Focus Courses Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>Fall</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Spr</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Electives</strong></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Fall</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Spr</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Cost Per Credit Hour

<table>
<thead>
<tr>
<th></th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Annual Salary</td>
<td>64,190</td>
<td>64,500</td>
<td>66,000</td>
<td>68,750</td>
<td>71,500</td>
</tr>
<tr>
<td>Benefits</td>
<td>32,464</td>
<td>34,500</td>
<td>36,750</td>
<td>39,200</td>
<td>42,000</td>
</tr>
<tr>
<td>Total Comp Cost</td>
<td>97,654</td>
<td>100,000</td>
<td>103,750</td>
<td>108,150</td>
<td>113,500</td>
</tr>
<tr>
<td>Cost Per Credit Hour</td>
<td>4,076</td>
<td>4,096</td>
<td>4,116</td>
<td>4,136</td>
<td>4,156</td>
</tr>
</tbody>
</table>

### Computer Science Direct Course Compensation Costs

<table>
<thead>
<tr>
<th>Focus Courses</th>
<th>#Credits</th>
<th>Total Compensation Costs (salary + benefits)</th>
<th>Current assumption: no incremental direct overhead costs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fall</td>
<td>1</td>
<td>10,579</td>
<td>10,800</td>
</tr>
<tr>
<td>Spr</td>
<td>1</td>
<td>10,579</td>
<td>10,800</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1</td>
<td>10,579</td>
<td>10,800</td>
</tr>
<tr>
<td>Electives</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fall</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Spr</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Other Direct Costs

| Virtual Env             | 159     | 2,379                                        | 8,044                                                  |
| Other Items?            |         |                                              |                                                        |
| **Total**               | 159     | 2,379                                        | 8,044                                                  |

### Contribution Margin

|                         | 807 | (1,571) | (2,198) | (6,205) | (8,108) | 1,062 | (6,805) | 6,398 | (692) | 12,308 |

### Direct Overhead Costs

|                         | (763) | (8,403) | (7,046) | (408) | 11,615 |

### CM after Direct Ovhd

|                         | 807   | (1,571) | (2,198) | (6,205) | (8,108) | 1,062 | (6,805) | 6,398 | (692) | 12,308 |

### Indirect Ovhd

|                         | 6,427 | 7,952 | 17,918 | 39,294 | 45,478 | 44,678 | 37,085 | 50,925 | 43,198 |

### Operating incr/(decr)

|                         | (5,620) | (9,522) | (20,116) | (25,508) | (41,062) | (24,427) | (51,483) | (30,687) | (51,617) | (30,890) |

### Memo:

- Gen Ed & Elective Credit Hours: 180, 146, 304, 252, 436, 370, 592, 489, 725, 599
- Gen Ed & Elective Revenue: 49,060, 39,738, 82,894, 68,719, 118,810, 100,715, 161,323, 133,398, 197,566, 163,367
- Totals By Year: 12, 23, 35, 49, 60
- 2016: 12, 23, 35, 49, 60
- 2017: 419, 776, 1,171, 1,623, 1,988
- 2018: 94, 195, 315, 443, 542
- Lecturer 3 per credit hour: 1,232
- Benefits: 95
- Cost Per Credit Hour: 7.7%