Preliminary Report of the
University of Massachusetts
Cybersecurity Task Force

December 2014

D. Banks, UMSO
W. Burleson, UMA
J. Chen, UML
P. Chen, UMB
L. Clarke, UMA
B. Coleman, UMW
J. Cunningham, UMSO
J. Dubach, UMA
J. Kurose, UMA
L. Fiondella, UMD
X. Fu, UML
W. Johnson, UML
J. Krishnamoorthy, UMB
K. Lapane, UMW
H. Liu, UMD
A. Mehta, UMB
T. Meressi, UMD
K. Subbaswamy, UMA (chair)
J. Wang, UML
J. Wileden, UMA
L. Wilson, UMSO
I. Introduction

“Cybersecurity” is an issue that continues to make all the wrong kind of headlines in the press: Snowden and the NSA, New York Times reporting “Russian Hackers Amass over a Billion Internet Passwords”, massive exposures of credit card information at Target and Home Depot. All sectors of society and the economy have been impacted, including higher education with, for example, major data breaches reported at Indiana University and the University of Maryland earlier this year. UMass campuses have not been spared and we repel external attempts to crack our systems on a nearly continuous basis.

Our nation’s cybersystems have rapidly transformed nearly every sector of society. Increasingly, they monitor and control our energy distribution, transportation, and telecommunication networks, as well as our public and private buildings; they power commerce and financial services; they carry entertainment and critical information services; and they touch us individually through our personal devices and data (e.g., cars, phones, glasses, and health systems). And yet this expansion has also exposed the fragility and vulnerability of these systems to both misuse and attack. Cybersecurity and privacy have become critical issues in our information-driven and knowledge-based economy.

There is little doubt that these issues will remain critical for years to come and that Massachusetts industry has both the need to address them in its current operations as well as the capability to become a greater force in this ever-growing segment of the modern economy. The University of Massachusetts can and should muster and expand its resources, both in education and research, in order to support the Commonwealth and the region as the University’s land-grant origin and mission would demand.

Therefore, at the behest of President Caret, the Cybersecurity Task Force was formed in late Fall of 2013 to assess the University’s academic capabilities in the area of cybersecurity, to understand how the University is positioned in this area within the Commonwealth and region as well as what it would take to move forward, and to make recommendations on next steps in this direction. To be
clear, the robustness of the system-wide IT infrastructure is not within the purview of this Task Force.

The Task Force’s activities took two parallel directions. Internally, it focused on compiling an inventory of existing instruction and research related to cybersecurity, understanding industry standards for skills evaluation in cybersecurity, and developing ideas/proposals for expanding these activities in support of the business sector. Externally, the Task Force reviewed and provided input to the Business Higher Education Forum (BHEF) development of a proposal funded by the Gates Foundation. The scope of the proposal was to plan for the expansion of BHEF’s CyberUP program initially deployed in Maryland and supported by industry partners (particularly, Northrup-Grumman), in a number of ways, including establishing a “Massachusetts Cyber Network” similar to the Maryland effort but modified as appropriate for the needs and resources within the Commonwealth of Massachusetts. Key elements of this proposal are summarized in Appendix I.1. The Task Force also reviewed a related report from Burning Glass presenting an assessment of Massachusetts cybersecurity workforce need, educational/training requirements for relevant positions, etc.; a brief summary of results is presented in Appendix I.2.

Consistent with the University’s mission, there are three components to the Report, covering education (workforce development), research, and outreach to industry.

II. Workforce Needs

There is a tendency to think of cybersecurity as a highly technical issue requiring advanced technical skills. While this is certainly one aspect of the cybersecurity issue, the pervasiveness of the issue demands a broader education effort as well. Thus, any instructional/curricular developments should address both the need to develop “cyber enabled” staff (i.e., the technical front line combatants) and the need to spread “cyber awareness” across the many disciplines that encounter cybersecurity issues. Not surprisingly, this calls for instruction at a variety of levels, as discussed below. In many cases, those specializing in cybersecurity often require foundational background in computer science and engineering, mathematics, law, and other “traditional” academic disciplines.
II.A Certificate Programs

There are at least two basic approaches to “certifying” an individual’s skill/prowess in cybersecurity. The first approach focuses on the individual, with the certification usually achieved by passing one or more examinations administered by a professional organization. A list of some of the more respected certificates (as determined by a competition sponsored by SC Magazine and judged by a panel of approximately thirty industry CEOs, CSOs (chief security officer), and CISOs (chief information security officer)) is attached in Appendix II.A.1. From the University’s point of view, these provide suggestions for subject matter to be included in any cybersecurity curriculum, but it remains up to the individual to prepare for and take the appropriate certificate examination.

Training materials/courses for those who wish to take professional certificate examinations such as Certified Information Systems Security Professional (CISSP: see Appendix II.A.1) are available from both not-for-profit and for-profit vendors/institutions.

II.B Undergraduate Programs

The second approach focuses on the academic program at the institutional level and is more akin to an “accreditation” wherein certification is granted to a program and, therefore, individuals going through such a program can claim the certification. The leading agencies in this approach are the National Security Agency and the Department of Homeland Security who have jointly defined the requirements for designation as a “Center of Academic Excellence” (CAE). There are three such centers of relevance to UMass: CAE-2Y, intended primarily for Community College programs but which would be part of an articulation agreement for students moving from a Community College into a four-year UMass program (as would be relevant for our ABLE4STEM program); CAE-IA/CD (Information Assurance/Cyber Defense), matching to a four-year curriculum; and CAE-R, certifying research efforts in the field of cybersecurity. Some of the requirements for and benefits from a CAE accreditation are given in Appendix II.A.2. ABLE4STEM will connect Community Colleges offering AS or certificate cyber tracks with emerging UMass certificate/degree programs in cyber IA/CD. As a model program in an NSF-funded BHEF project, ABLE4STEM will support course
development and 2+2 curricular articulations. As a first connection, Middlesex CC and UMass Lowell are participating. MCC created an IT transfer program focused on network security administration that conforms to the framework established jointly by the National Security Agency and the Department of Homeland Security. UMass Lowell and MCC are reviewing alignment and articulation with Lowell's emerging bachelor's program. This should serve as a prototype for similar articulation arrangements between other Community Colleges and UMass campuses.

As mentioned above, cybersecurity education goes well beyond the “cyber enabled” but can and should touch, and in many cases be founded upon, many other disciplines. Undergraduate education in cyber-security can be accomplished in many ways, ranging from cybersecurity “minors” with a major in another cognate discipline, to certificate preparation curricula available to all undergraduates, to dedicated courses, perhaps team-taught among faculty from multiple departments and/or industry collaborators, in the disciplines (e.g., computer science and engineering, management) where cybersecurity is a particularly relevant topic. We expect this curriculum to continually and rapidly evolve over the next few years, particularly as we establish greater communication and cooperation with industry partners. Most, if not all, of these courses could be delivered through UMassOnline as needed.

II.C Graduate Programs

For the most part, graduate education in cybersecurity will focus on the experts (the “cyber enabled”) in specific disciplines and, like much of graduate education, will be strongly coupled to the research efforts in the relevant departments. However, in Management and other MBA programs, options should be made available for one or more courses providing “cyber awareness” to students who may likely find themselves confronting cybersecurity issues in their subsequent employment. A similar need may exist in other graduate programs; these should be identified as we move forward.

II.D Current Status/Plans

Amherst: School of Computer Science (SCS) and ECE (Electrical and Computer Engineering) Department faculty teach a variety of foundational courses at both

Boston: Two introductory forensics courses and upper level undergraduate courses are in place at UMB. The Dept. of Computer Science is setting up a cybersecurity instruction lab to be used both for instruction and for training student cybersecurity teams. Additionally, Prof. Chen, Dept. of Engineering, received a NSF grant “Enriching Security Curricula and Enhancing Awareness of Security in Computer Science and Beyond” aimed at addressing the critical shortage of qualified IA professionals in the nation’s workforce. Work includes updating the security curricula to include essential and incorporating hands-on and interactive courseware. See Appendix II.D.Boston for more detail.

Dartmouth: UMass Dartmouth is developing a curriculum and some new courses that will match the Knowledge Units required to designate the campus as NSA/DHS National Center of Academic Excellence (CAE) in Information Assurance/Cyber Defense (IA/CD). It includes SANS Critical Controls and aligns with the new IEEE Computer Engineering Body of Knowledge. Based on an internal assessment, it has been concluded that the curriculum, with some updates currently being made, will satisfy CAE-IA/CD Program Requirements. See Appendix II. D. Dartmouth for specifics.

Lowell: UMass Lowell offers a number of IT and professional programs with cybersecurity elements. These include courses offered through the Department of Computer Science, the Division of Online and Continuing Education, the Department of Electrical and Computer Engineering, the School of Criminology
and Justice Studies, and the Manning School of Business. Complete descriptions of these programs can be found at [http://ccf.cs.uml.edu/?q=node/38](http://ccf.cs.uml.edu/?q=node/38). Appendix II.D.Lowell lists cybersecurity specific courses. As mentioned above, UMass Lowell is engaging Middlesex Community College in developing articulation agreements for cybersecurity programs. Lowell is also in the process of applying for CAE-IA and CAE-R designations.

### III. Research

Cybersecurity is far from a static subject. It is probably changing more rapidly than the underlying technology itself, a technology which is known for its rapid rate of change. As such, any instructional program in cybersecurity must be accompanied by an appropriate research effort. Fortunately, the UMass campuses are already highly engaged in such research. Appendix III.Amherst, Appendix III.Boston, Appendix III.Dartmouth and Appendix III.Lowell provide brief descriptions of the broad variety of relevant research.

### IV. Next Steps

BHEF suggested that a “MA Cybersecurity Network will be a vehicle to bring together academic, industry and other key partners to help stand up new and bolster existing cybersecurity education programs at UMass institutions to meet the growing demand for cybersecurity professionals.”

It should be clear, and is certainly borne out by the Maryland experience, that a cybersecurity program that successfully delivers what the Commonwealth’s and region’s industries need requires close collaboration, cooperation, and consultation with those industries. While the Task Force recognized this immediately, it also realized that we started the Task Force’s activities in somewhat of a “chicken and egg” position; namely, it would be difficult to approach the relevant industrial sectors until we had established a clear definition of what the University had to offer them. With the efforts of the past year along with additional programs currently under development, the Task Force believes the University is now positioned to approach a broad spectrum of potential industrial partners and potential industrial consumers of the cybersecurity instructional and research programs it can offer.
This is not to say that efforts to date have been devoid of industry support, input, and advice. Indeed, the MACP provided seed funding to get the ABLE4STEM program started. Members of the Task Force interviewed David Saul, Chief Scientist and former CISO, and Mark Morrison, current CISO at State Street about corporate needs in the area of cybersecurity both in terms of the magnitude of need and in terms of the type of education/training required. Mandy Andress, Assistant Vice President for Information Risk Management at MassMutual, has consulted with Professor Fu at UMass Lowell and Professor Hong Liu at UMass Dartmouth to bring industry perspective to the newly developing curricula.

But now is the time to seek broader industry participation. Two near-term opportunities have presented themselves:

- A representative of the MACP participated in the meeting of the Task Force where this draft report was discussed.
- The BHEF will hold its annual meeting in Boston on the UMass Boston campus December 1st and 2nd. This should provide an excellent opportunity for the University to showcase to a wide audience its programs in cybersecurity.

However, the Task Force feels that, in order to fully establish the necessary liaisons with a broad spectrum of relevant industries, the University must name an individual or establish a position, presumably in the System Office, to shepherd the development of industrial contact and participation and coordinate University activities. While individual campuses and individual faculty can network with counterparts in individual companies, the broader partnerships the Task Force envisions require coordination and communication across the University. The Task Force is not in a position to determine if this requires a new hire or if it can be incorporated into the portfolio of an existing staff member. It would, however, be highly encouraging if at least partial funding for this coordinator position could be obtained from corporate partners, if only in a short-term, seed money, arrangement.

The Cybersecurity Task Force, intended as an ad hoc body, would go out of existence but the above-named coordinator should establish an advisory committee with representation akin to the composition of the Task Force.
Finally, the Task Force suggests the University establish a semi-annual “Cybersecurity Forum” to be hosted on a rotating basis on each of the campuses (and perhaps on industry sites) to provide the opportunity for the campuses to share information among themselves but also to invite industry partners to address the University cybersecurity community. The above-named coordinator and his/her advisory committee would organize these Forums.

V. Recommendations

The following specific recommendations are intended to launch a leadership role for the University of Massachusetts that attends to the cybersecurity needs of the Commonwealth and contributes significantly to the work of research universities nationwide. These initial steps themselves require an infusion of substantial resources and the larger role envisioned for the University requires collaborations with other universities and colleges together with partnerships that leverage the capabilities and resources of industry, foundation, and government sectors.

1: Make CISSP curriculum materials available to the public via UMass Online. Since these are standard materials leading up to a uniform professional exam, there need only be a single instance of this managed by a single campus (or by UMOL).

2: The Boston, Dartmouth, and Lowell campuses of UMass, which either already have, or are planning to apply for CAE designation, should be encouraged to obtain/maintain such designation. They should be supported to develop full curricula for the 4-year degree as needed. The appropriate 4-year degree programs should also be made available at the Springfield Center. Scholarships designed to attract high quality students to these programs should be established.

3: The Amherst Campus should be supported to further strengthen the cybersecurity components/tracks within its existing degree programs, and to develop new programs as needed, across the wide range of areas (computer science and engineering, social sciences, business) that are foundational to a cyber-security education.

4: The various programs across the campuses should also be coordinated to better complement each other, be developed to help meet the workforce needs of the
Commonwealth, be marketed widely within the Commonwealth, and have scholarships established (e.g., through programs such as NSF CyberCorps, industry support) to attract students to the programs. Given the critical need for cyber-security specialization within the Commonwealth and beyond, the aim should be to at least double the number of students graduating from these programs over five years.

5: The UMass campuses and MA public Community Colleges, working through ABLE4STEM, should partner to obtain CAE-2Y designations at the CCs and create transfer pathways into UMass CAE certified 4-year degree programs. Such a transfer pathway should be made available at the Springfield Center as well.

6: A system-wide center for cybersecurity research (UMCCCR), analogous to the Center for Clinical Translational Science, should be established, with one campus designated as the lead campus and an executive committee with representatives from all campuses. Support should be made available, on a competitive basis, for research assistantships, post-doctoral positions, and seed funds.

7: The President should create a Massachusetts cybersecurity industry-education network (MCIEN) advisory board to advise the system regarding workforce needs, curricular design and articulation, and research areas. This should follow the structure proposed by the BHEF planning work done under the Gates grant in collaboration with UMass. This effort should be coordinated with the Massachusetts Advanced Cyber Security Center (ACSC).

8: A liaison position for the Massachusetts cybersecurity industry-education network should be established in the President’s office. Among other responsibilities, the MCIEN liaison should work to create internship and job opportunities for students across the system in the cybersecurity sector.

Addendum from the Task Force Chair

Here is a brief summary, per the Task Force Chair, of several themes that emerged from the BHEF National Meeting on Cybersecurity held on the UMass Boston campus Dec. 2nd:
The Burning Glass study documented the demand for jobs with a cybersecurity component, but the needed qualifications were not clear that data mining. There was debate and disagreement about the adequacy of industry specified certification such as CISM. While there was acknowledgment that such certification was a common factor that recruiters looked for, Chief Information Security Officers present at the meeting, gave a very different picture of what the CISO's were looking for. Here is a summary of themes that were heard repeatedly:

1. We need a medley of qualifications: people who can think, interact with people, who are problem-solvers.
2. People trained in an interdisciplinary way with a combination of technical and risk-management skills.
3. People who can do cybersecurity in a regulatory environment (compliance with national and international regulations)
4. Students should get deep first (in something) before getting broad.
5. People who are trained to block and tackle, who can look around corners.
6. Remember we are counteracting nation-states who are putting unlimited resources to attack. We need to counter smartly, without that kind of human capital.
7. Applicants should have intelligence mindset, data analytics background, data forensics capability, and practical skills (internship).
8. Security analytics, usage pattern analytics, project management skills.
9. Systems science, systems learning,
10. Data analytics, data forensics, intelligence & operations, threat assessment (soft skills).

In summary, it appears as though a combination of technical skills surrounding data and networks, as well as soft skills such as critical thinking, project management, and threat assessment, along with in-house training is what is needed. The training of security professionals and security-aware professionals will evolve in the years to come. This should happen in a collaborative environment between universities and industry so that the supply matches demand not only in numbers, but also in the knowledge and skill sets.

There is also a recent congressional testimony from one of the Task Force Members (Jim Kurose) which speaks to the cybersecurity needs which is helpful in
Appendix I.1 Excerpts from BHEF “CyberUP” Proposal

The BHEF CyberUP strategy identifies five areas of opportunity: (1) Share best practices, inform policy, identify workforce needs and develop national competency frameworks verifying the three pillars of academic experience, work experience, and certifications; (2) Launch a Greater Washington Area network to share evidence-based practices, inform policy, and scale CyberUP programs to new institutions in the Greater Washington area; (3) Use evidence-based practices developed through Maryland to launch a Massachusetts cyber network to share best practices, inform policy, and bring CyberUP programs to the state; (4) Strengthen the BHEF-USM Network role and scale CyberUP programs to new University System of Maryland institutions; (5) Increase quality of existing programs to codify best practices including partner ecosystem, engaging more companies, and addressing low-income student needs.

BHEF’s stated vision for the program: At the college/university, regional and national levels, BHEF builds on cybersecurity learnings and convenes business leaders to develop industry-recognized cybersecurity competency map(s), expand regional partnerships, and develop industry-certified courses and programs.

Translating key findings into potential implications for a program design:

- CyberUP should encourage programs to incorporate early outreach into talent pipeline strategies
- BHEF should work with employers to further define cybersecurity-enabled and cybersecurity-aware professionals and the business demand for these individuals
- Both foundation and technical skillsets should be addressed in CyberUP programs
- A focus on internships and securing work experience early in the academic setting should be a focus of CyberUP
- Depending on the industry sector of focus and relation to federal contracts, certification(s) may be an effective outcome of a program
- BHEF should focus on programs that include Bachelor’s degrees with two-year on-ramps
• Cybersecurity-related work experience should be a critical component of a program if cybersecurity specialists are the target workforce

Key components of the CyberUP program:

• Once strategy and goals are determined, the framework helps partners design a project to recruit, prepare, and place students in alignment with employer demand and student needs.

• While some decisions are more focused on the academic, student, or employer perspective, it is important for decisions to be made with input from all relevant parties within the partnership ecosystem and based on the strategy developed by the partner ecosystem.

• Decisions should be driven by market demand and within the specific context of each college/university project. Where applicable, BHEF offers guidance based on evidence-based lessons.

• Throughout the planning process it is important to consider the unique needs and constraints of each project to best address low-income student barriers for entry and persistence, and the appropriate combination of academic coursework, work experience, and certifications to prepare students to meet businesses’ demands.
Appendix I.2  Key Findings from the Burning Glass “Report on Cybersecurity Jobs in MA”

Burning Glass Technologies, drawing from its database of over 100 million online job postings, analyzed postings with cybersecurity related titles in 2013 in order to quantify the overall demand for cybersecurity professionals in Massachusetts and detail the skills and qualifications Massachusetts employers request. The key findings:

- There were 7,129 postings for cybersecurity-related jobs in Massachusetts.
- Cybersecurity postings in Massachusetts have grown twice as fast as IT postings overall.
- On a per capita basis, Massachusetts has the 4th highest concentration of cybersecurity postings in the nation, behind only Virginia, Maryland, and Colorado.
- Most common positions posted carried titles such as Security Engineer, Information Assurance Engineer, Data Security Administrator, Information Security Manager, IT Security Analyst, Cyber Intelligence Analyst.
- The demand by industry sector (% of postings) in Massachusetts: Professional Services (38%), Finance and Insurance (12%), Manufacturing & Defense (11%), Information (9%), Health Care (7%), Educational Services (7%), Other (16%). Massachusetts demand was higher in Health Care and Educational Services than nationwide and lower in Manufacturing & Defense.
- 97% of postings prefer or require a Bachelor’s degree; 89% require a Bachelor’s degree; 26% prefer or require a Master’s or above.
- 44% of all cybersecurity positions in Massachusetts request at least one certification; the most frequently requested certifications include CISSP (23%), CISA (17%), and CISM (7%) [see Appendix II.A.1].
### Appendix II.A.1: Selected Professional Certificates

**SC Magazine – 2014 Best Professional Certification Programs:** Programs are defined as professional industry groups offering certifications to IT security professionals wishing to receive educational experience and credentials. Entrants can include organizations in the industry granting certifications for the training and knowledge they provide.

<table>
<thead>
<tr>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GIAC - Global Information Assurance Certification for GIAC Intrusion Analyst (GCIA)</td>
<td>The GIAC Intrusion Detection In-Depth (GCIA) was created to provide assurance that a certified individual holds the appropriate level of knowledge and skill necessary for anyone relied upon by an organization to perform intrusion detection using network and host-based techniques. A holder of the GCIA credential is certain to have a complete understanding of network protocols, traffic and network theory, including normal and malicious fragmentation, abnormal stimulus response, and TCP/IP fundamentals. They are familiar with attacks against NIDS, computer systems and the network infrastructure. They are able to analyze common network traffic patterns and dig into packets when more information is needed.</td>
</tr>
<tr>
<td>GIAC Security Essentials</td>
<td>The GSE certification is the most prestigious in the IT Security industry. The current exam was developed by subject matter experts and top industry practitioners. The GSE’s performance based, hands-on nature sets it apart from any other certifications in the IT security industry. The GSE will determine if a candidate has truly mastered the wide variety of skills required by top security consultants and individual practitioners. The GSE exam has two parts: <strong>Part 1: Multiple Choice Exam:</strong> The current version of the GSE multiple choice exam has the passing score set at 75% and a time limit of 3 hours. Passing this exam qualifies a person to sit for the GSE hands-on lab. <strong>Part 2: 2-day GSE Lab exam:</strong> Day 1 of the GSE lab consists of an incident response scenario that requires the candidate to analyze data and report their results in a written report. Day 2 consists of a rigorous battery of hands-on exercises.</td>
</tr>
<tr>
<td>Guidance Software for EnCase Certified Examiner (EnCE)</td>
<td>The EnCase® Certified Examiner (EnCE®) program certifies both public and private sector professionals in the use of Guidance Software's EnCase® computer forensic software. EnCE® certification acknowledges that professionals have mastered computer investigation methodology as well as the use of EnCase® software during complex computer examinations. Recognized by both the law enforcement and corporate communities as a symbol of in-depth computer forensics knowledge, EnCE certification illustrates that an investigator is a skilled computer examiner.</td>
</tr>
<tr>
<td>Certified Information Systems Auditor (CISA)</td>
<td>The Certified Information Systems Auditor (CISA) is a certification issued by the Information Systems Audit and Control Association (ISACA). In order to receive the certification, applicants must pass an examination that includes sections on the following topics: auditing practices and techniques, gathering and preserving evidence in forensic investigations, control objectives and reporting techniques. Before an applicant is allowed to sit for the exam, he or she must already have a minimum of five years of experience in one of five information systems of expertise: Information Systems (IS) audit process, IT Governance, Systems and Infrastructure Lifecycle Management, IT Service Delivery and Support, Protection of Information Assets.</td>
</tr>
<tr>
<td>Certified Information Security Manager (CISM)</td>
<td>The Certified Information Security Manager (CISM) is a top credential for IT professionals responsible for managing, developing, and overseeing information security systems in enterprise level applications, or for developing best organizational security practices. The CISM credential targets the needs of IT security professionals with enterprise level security management responsibilities. Credential holders possess advanced and proven skills in security risk management, program development and management, governance, and incident management and response.</td>
</tr>
<tr>
<td>Certified Information Systems Security Professional (CISSP)</td>
<td>The Certified Information Systems Security Professional (CISSP) is an advanced level certification for IT professionals serious about careers in information security. Offered by the International Information Systems Security Certification Consortium (ISC)², this vendor neutral credential is recognized world-wide for its standards of excellence. The CISSP continues to be highly-sought after by IT professionals, well recognized by IT organizations, and a regular fixture on most-wanted or must-have security (and other) certification surveys. A minimum of 5-years of experience in at least two of ISC²’s ten common body of knowledge (CBK) domains is required for this certification. CBK domains include Access Control, Application Development Security, Business Continuity and Disaster Recovery Planning, Cryptography, Information Security Governance and Risk Management, Legal Regulations, Compliance and Investigations, Operations Security, Physical Environmental Security, Security Architecture and Design, and Telecommunications and Network Security.</td>
</tr>
</tbody>
</table>
Appendix II.A.2: Requirement for and benefits from CAE designation

1) Requirements for CAE Designation (For CAE-IA/CD Program)
   - Letter of intent from executive
   - Outreach / Collaboration
   - Center for IA/CD Education (website)
   - A robust and active IA/CD academic program
   - IA/CD is multidisciplinary within the institution (alignment with IT)
   - Practice of IA encouraged throughout the institution (awareness)
   - Student based IA/CD Cybersecurity research
   - Number of IA/CD/Cybersecurity faculty and course load
   - Faculty active in current IA/CD/Cybersecurity practice and research

2) Benefits of CAE Designation
   - Academic standard (minimum requirements) – 138 institutions meet these standards
   - Federal grant and student scholarship opportunities – Moraine Valley College (Illinois) received over $20 M in grants
   - Academic partnership opportunities – 7 courses from Moraine Valley Community College have been made public
   - Industry partnership opportunities – Establish academic advisory committee
   - Collaboration – Create a community collaboration – share content among higher education institutions
Appendix II.D. Amherst: Educational Activities

As noted in Section II.D, faculty in the UMass Amherst School of Computer Science (SCS) and in the Department of Electrical and Computer Engineering (ECE) teach a variety of foundational courses at both the undergraduate and graduate levels in security, privacy, and forensics; a sampling of these courses are listed below. A Security & Privacy track ([http://www.cs.umass.edu/ugrad-education/information-assurance](http://www.cs.umass.edu/ugrad-education/information-assurance)) is available through the SCS BS and BA degree programs. As also noted in Section II.D UMass School of Computer Science often appears in lists of top universities, nationwide, for a computer science degree with a focus in cybersecurity. SCS and ECE faculty complement classroom educational activities with research mentoring of graduate and undergraduate students in cybersecurity, with than 10 million dollars jointly in research funding in cybersecurity since 2011 (see Appendix III).

A sampling of courses in security and privacy offered on the Amherst campus:

- ECE 597LL/697LL Trustworthy Computing
- ECE 597AB/697AB Security Engineering
- ECE 597XX/697XX Cryptography Algorithms
- ECE 597CR/697CR Cryptography Engineering
- ECE 597ES/697ES Embedded Systems Security
- CMPSCI 365 Digital Forensics
- CMPSCI 391LI S-Computer Crime Law
- CS 460: Intro to Computer and Network Security
- CMPSCI 466 Applied Cryptography
- CMPSCI 660 Advance Information Assurance
- CMPSCI 691DP: Seminar - Principles of Data Privacy

Details about these courses can be found at [http://www.cs.umass.edu/ugrad-education/information-assurance](http://www.cs.umass.edu/ugrad-education/information-assurance) and [http://ece.umass.edu/](http://ece.umass.edu/)
Appendix II.D. Boston: Educational Activities

1.1. Courses
- IT 220: Computer Forensics I
- IT221: Computer Forensics II
- IT420: Network and Mobile Forensics
- IT 421: Digital Forensics & Malware Analysis
- IT 443: Network Security Administration
- MSIS 428 Information Security
- MSIS 613: Information security, Privacy, and Regulatory Compliance
- MSIS 623: Network and Mobile Forensics
- MSIS 624: Digital Forensics/Malware Analysis
- MSIS 627: Business Computer Forensics and Incident Response
- MSIS 634: Health Information Privacy & Security
- CS 449: Introduction to Computer Security
- Computer and Information Security: a special topic graduate-level course
- Advanced Topics in Data Security and Privacy (in development)

1.2. Instruction Lab
Dr. Ghinita at Dept. of CS is setting up a cybersecurity instruction lab at Department of Computer Science, which will be used both for instruction, as well as for training student cybersecurity teams.

1.3. Grant
Dr. Chen of the Department of Engineering received a NSF grant “Enriching Security Curricula and Enhancing Awareness of Security in Computer Science and Beyond” (award # 1423915). This project is aimed at addressing: (i) the critical shortage of qualified IA professionals in the nation’s workforce by training faculty nationwide to increase security topics in their courses in computer science and beyond in other STEM disciplines, (ii) the much-needed update of security curricula to include essential techniques from machine learning, data mining, natural language processing and statistics, and (iii) the dearth of hands-on and interactive courseware for security and especially privacy in emerging domains and challenges.

1.4. Cybersecurity meeting and competitions
- UMB will host Business-Higher Education Forum’s National Cybersecurity Network meeting in 12/14.
- Training UMass Boston Cybersecurity Team. Dr. Ghinita is currently training the UMB CS team to regularly participate in inter-collegiate events such as the regional Northeastern National Collegiate Cyber Competition (NECCDC). In NECCDC 2014, the UMB’s student team was ranked 2nd by the Red Team for their ability to defend against cyber-attacks, and in 6th place overall out of 10 teams. Dr. Ghinita also trained students for the Massachusetts Governor’s CyberAces competition. Out of the total 79 participants who qualified for the final CyberAces round, five were UMB students.
- Organizing Cybersecurity competitions. UMass Boston co-organized the Massachusetts Governor’s First CyberAces Competition in cooperation with the CyberAces foundation (www.cyberaces.org), a
SANS Institute-sponsored foundation that creates partnerships with various state and federal level government bodies to advance the formation and training of cybersecurity professionals. The 2013-14 inaugural edition was held at UMB, on May 3rd 2014.

**Appendix II.D. Dartmouth: Educational Activities**

Approved by the Electrical and Computer Engineering (ECE) Department following the recommendation by its Computer Engineering (CPE) Curriculum Committee, UMass Dartmouth took a holistic approach to cybersecurity curriculum development. The CPE curriculum matches the Knowledge Units required to be designated as an NSA/DHS National Center of Academic Excellence (CAE) in Information Assurance/Cyber Defense (IA/CD). The curriculum also includes SANS Critical Controls and adapt to the new IEEE Computer Engineering Body of Knowledge. Based on initial assessment involving fifteen faculty and staff (listed below), the campus is at a stage where it will satisfy the CAE-IA/CD Program Requirements with some action items in progress. The Cybersecurity Curriculum Initiation Funding from UMass President’s Office is being used to support a student assistant who will help promote cybersecurity education and research.

UMass Dartmouth offers the following three cyber-security related courses. **ECE 489/549 Network Security**, **CIS 477 Computer and Information System Security**, and **ECE 4xx/5xx Cyber Threats and Security Management**. The Cyber Threats and Security Management course was run as a pilot course in Spring 2014. It has since been approved by the CPE Curriculum Committee and the ECE Department and is now awaiting approval by the College of Engineering Curriculum Committee.

- **Faculty:**
  - **Costa, Antonio H.** Professor and Chair of Electrical and Computer Engineering: Mixed time-frequency representations, spectral estimation, signal processing.
  - **Fiondella, Lance** Assistant Professor of Electrical and Computer Engineering: Reliability and security engineering, transportation engineering.
  - **Fortier, Paul J.** Professor of Electrical and Computer Engineering: Database systems, real-time systems, computer architecture, networks, sensor/embedded systems and security, database security.
  - **Liu, Hong** (Graduate Program Director beginning January 2015) Professor of Electrical and Computer Engineering: Computer networks, network security, compilers and programming languages.
  - **Michel, Howard E.** Associate Professor of Electrical and Computer Engineering: Distributed artificial intelligence, artificial neural networks, distributed computing, computer vision, computer networks.
  - **Viall, Philip H.** Professor of Electrical and Computer Engineering: Computer networking, assembly languages, rehabilitation engineering, computer security.
Wang, Honggang Assistant Professor of Electrical and Computer Engineering: Wireless health, wireless networks, multimedia communication, multimedia & cyber security, sensor networks & cyber-physical system.

Xing, Liudong Professor of Electrical and Computer Engineering: Reliability and security engineering, network reliability, fault-tolerant computing, risk assessment.

Xu, Haiping Associate Professor of Computer and Information Science: Distributed software engineering, formal methods, mobile cloud computing, cybersecurity, multi-agent systems, and semantic web.

Gunasekaran, Angappa Dean of Charlton College of Business and Professor of Management Information Systems.

Hsieh, Tien-Shih Assistant Professor of Accounting and Finance.

Shea, Timothy Associate Professor of Management Information Systems

Sulkowski Adam J. Associate Professor of Business Law.

- Staff
  Oliveira, Craig R. Associate Director of Enterprise Systems and Security: Ensuring security, integrity, and reliability of enterprise systems and operations.
  Sullivan, Brian M. Enterprise Systems Project Manager: Data loss protection, training and education using SANS 20 Controls as guidance for security.
Appendix II.D. Lowell: Educational Activities

Department of Computer Science  Computer security and forensics related courses:

91.661 Advanced Topics in Network Security
91.530 Special Topics: Digital Forensics
91.460 Special Topics: Digital Forensics
91.561 Computer & Network Security I
91.562 Computer Security II

Division of Online and Continuing Education

a. The Graduate Certificate in Network Security. See
http://www.continuinged.uml.edu/online/certificates/networksecurity.cfm

94.561 Computer Network Security
94.562 Digital Forensics
94.563 Secure Mobile Networks
94.543 Intrusion Detection Systems

b. Online Master of Science in Information Technology (MSIT). All the courses for the Graduate Certificate in Network Security are incorporated into the MSIT program in case students want to pursue MSIT, which is offered by the UMass Lowell Computer Science Department in collaboration with the Division of Online and Continuing Education. This contemporary degree is technically-focused and features cutting-edge knowledge content critical to the workforce needs of the IT industry.

Department of Electrical and Computer Engineering

16.658: Computer Network Security

Manning School of Business

MIST.770 Information Privacy and Security
Appendix III. Amherst: Research Activities

Security and Privacy Research Activities on the UMass Amherst Campus

Researchers in the School of Computer Science and the Dept. of Electrical and Computer Engineering are pioneering new techniques to make computer systems, networks and electronic devices more secure, and to protect privacy in an increasingly connected world. Among the areas of current research activity are the following.

Cybercrime. Prof. Brian Levine (CS) leads the Center for Forensics. The Center’s research has had substantial impact on Internet-based crimes against children, including child pornography trafficking and the rescue of abused children. Thousands of federal and state law enforcement investigators in the US and abroad have used their software in more than ten thousand cases. Massachusetts State Police have called the project “unsurpassed”.

Embedded Systems. Profs. Wayne Burleson (ECE) and Christof Paar’s (ECE) are involved in many aspects of securing the "Internet of Things", including cryptographic solutions ranging from RFID tags to electric cars. They are also active in the area of hardware security, including the design and detection of hardware Trojans. Prof. Paar is co-founder of the leading hardware security conference CHES, as well as more specific workshops on RFIDSecurity, Automotive Security and Special Purpose Hardware for Cryptanalysis. And finally, Profs. Burleson, Paar, and John Collura (CEE) are developing novel anonymous payment systems that provide some information to the transportation system operator without divulging rider behavior and privacy.

Medical Devices. Profs. Wayne Burleson (ECE) and new faculty Daniel Holcomb’s (ECE) research includes securing implantable medical devices through lightweight hardware and protocols, thwarting potentially life—and threatening vulnerabilities and privacy disclosures. Holcomb uses formal methods and explores physiological sources of key material for medical devices. Burleson and Holcomb leverage the

“Cybersecurity” is a broad and evolving field, ranging from protecting the confidentiality, integrity, and availability of data, services, devices, and infrastructure; to ensuring the privacy of personal data carried in medical, governmental, and commercial settings; to ensuring secure communications across the Internet and cellular networks; to ensuring our rights are protected despite unprecedented sharing and analysis by companies and governments.
inherent variations and noise in modern CMOS circuits to support the lightweight cryptography that secures the Internet Of Things.

**Data Privacy.** *Prof. Gerome Miklau’s (CS) research focuses on the secure management of large-scale data, including: evaluating threats to privacy in published data; devising anonymization schemes for the safe publication of social networks, and audit logs; designing database management systems to implement security policies; and analyzing information disclosure. Miklau collaborates with Profs. Jim Kurose (CS) and Don Towsley (CS) on anonymization schemes for published network trace data.*

**Secure cryptographic devices.** *Prof. Israel Koren’s (ECE) research focuses on the analysis of side-channel attacks on hardware and software implementations of ciphers and the development of suitable countermeasures. Fault injection and EM attacks are studied and interactions between different types of side-channel attack are analyzed. Koren is co-founder of the "Fault Diagnosis and Tolerance in Cryptography Workshop (FDTC)" where the most recent theoretical and practical fault injection attacks and countermeasures are presented.*

**Securing Wireless Communications from Eavesdropping.** *Prof. Dennis Goeckel (ECE) develops methods that go beyond current cryptographic approaches to protect information transmitted in wireless environments from ever being decoded - even by an eavesdropper who can store the received signal and work indefinitely on it with infinite computational resources. In conjunction with Don Towsley (CS), he also considers the scaling properties of such approaches in large ad hoc wireless networks.*

**Covert Communications:** *Prof. Dennis Goeckel (ECE) and Don Towsley (CS) are also developing methods for communication when not just the content but also the mere presence of the communication must be hidden from a watchful adversary. In conjunction with Raytheon BBN in Cambridge, they have developed and demonstrated the first truly quantum-information-theoretically secure covert communication system that allows communication when all transmissions are prohibited.*

**Robust and Secure Mobile Networks.** The MobilityFirst project led by Profs. Arun Venkataramani (CS), Jim Kurose (CS), Don Towsley (CS), Prashant Shenoy (CS), and Michael Zink (ECE) is one of the four large-scale, NSF Future Internet Architecture projects. MobilityFirst is a clean-slate network architecture with user mobility, security, and robustness as core design principles.

**Mitigating Software Vulnerabilities.** *Prof. Emery Berger’s (CS) DieHard and DieHarder projects protect applications from as-yet unfixed bugs and security vulnerabilities that exploit them, acting as a new line of defense against hackers. This research has already led to improved security for millions of PC users, directly influencing key reliability and security features incorporated into Microsoft Windows 7 and 8.*

**Hardware Security.** *Prof. Sandip Kundu (ECE) researches hardware security primitives (HSP) for Internet of Things (IoT) devices and hardware Trojans. IoT devices cannot afford high-cost True Random Number Generators (TRNG), physically unclonable functions (PUF) and certified object authenticators (COA), yet they are more susceptible to differential power analysis (DPA), machine learning (ML) and spoofing attacks. IoT devices used in cameras, sensors for industrial and vehicular controls have been attacked at
an alarming rate, motivating the need for this work. Kundu’s hardware security research is funded by NSF and industrial collaborators include Intel and Freescale. Prof. Russ Tessier (ECE) and Prof. Christof Paar (ECE) have been working on securing FPGA designs against Trojan insertion. This goal is accomplished with obfuscation and the development of new encryption techniques which are difficult to break.

**Identifying Process Vulnerabilities.** Profs. Lee Osterweil (CS), Lori Clarke (CS), and George Avrunin (Math) are developing techniques for identifying vulnerabilities in key processes, such as those involved in preparing, carrying, and auditing elections. Their work uses a well-defined language to model election processes and then applies powerful analysis techniques to identify defects and vulnerabilities.

**Cloud Computing.** Prof. Yuriy Brun’s (CS) sTile project addresses a ubiquitous problem in cloud computing services: providers have access to user data. sTile allows the construction of software systems that distribute large computations onto the cloud, while providing guarantees that the cloud nodes cannot learn the computation’s private data.

**Web Security.** Prof. Arjun Gha (CS) works on fundamental security problems that arise in Web applications. These applications routinely incorporate code and data from untrustworthy third parties and thus open themselves to attack. His research has developed defenses based on strongly verifiable Web sandboxes.

**Censorship Resistance.** Newly joined Prof. Amir Houmansadr’s (CS) research addresses the threats posed by repressive regimes, corporations and advertising companies, and cybercriminals. His work involves building secure and privacy-preserving tools for Internet communications.

**A Partner of Choice**

School of CS faculty have received grants and gifts totaling more than 7 million dollars for research on security and privacy since 2011; in the ECE Department, faculty research grants in security and privacy had totaled more than 3 million dollars in that same time frame. The Center for Forensics partners closely with the FBI’s Cybercrime unit, the nationwide Internet Crimes Against Children Task Force, the Department of Justice, and MA and PA State Police. Other security and privacy-related research activities have involved BBN, BAE, Intel, and Microsoft, and federal funding from NSF and DARPA.
Appendix III. Boston: Research Activities

1. Research Activities

Here is a list of faculty working in the field of Cybersecurity and their projects.

- **Dr. Ramakrishna Ayyagari (Associate Professor, Management Information Systems)**
  - Disaster at a University: A Case Study in Information Security,

- **Dr. Noushin Ashrafi (Professor, Management Information Systems)**
  - Privacy protection via technology: Platform for privacy preferences (P3P)
  - Implementation of Privacy Protection Policies: An Empirical Perspective
  - Regulatory Privacy Practices in Europe

- **Dr. Ping Chen (Associate Professor, Engineering)**
  - Trustworthy evaluation of online resources
  - Identification of fake online reviews

- **Dr. Gabriel Ghinita (Assistant Professor, Computer Science)**
  - Privacy-preserving querying on encrypted data.
  - Security and Privacy for Provenance.

- **Dr. JongWoo Kim (Assistant Professor, Management Science and Information Systems)**
  - Incident-centered information security: Managing a strategic balance between prevention and response

- **Dr. Jean-Pierre Kuilboer (Acting Chair, Management Information Systems)**
  - Managing Network security
  - Online privacy policies: an empirical perspective on self-regulatory practices
  - Data privacy, US common practices

- **Dr. Bo Sheng (Assistant Professor, Computer Science)**
  - Security in near-field communications for mobile devices
  - Security protection against wireless jamming attacks
  - Secure and privacy-preserving queries in sensor networks and RFID systems
College of Engineering and Charlton College of Business faculty working on cybersecurity related research projects:

**Dr. Honggang Wang.** Assistant Professor of Electrical and Computer Engineering, recently received four National Science Foundation (NSF) research grants. One of them is to develop a physical-channel based lightweight authentication system for wireless body area networks. He has published more than 100 papers and won Best Paper Award in the 2008 IEEE Wireless Communications and Networking Conference. He serves as an Associate Editor of Wiley's Security and Communication Networks, IEEE Communication Magazine, IEEE Internet of Things, and IEEE Access Journal. He also serves as the TPC member for IEEE INFOCOM 2013-2015 and IEEE BSN 2014, and NSF panel 2012-2014.

**Dr. Lance Fiondella.** Assistant Professor of Electrical and Computer Engineering, has published nearly 60 peer reviewed journal and conference papers in reliability and security engineering. Four of his conference papers have been recognized with awards. His research is funded by the Department of Homeland Security. He serves as Vice-Chair of IEEE Standard 1633: Recommended Practice on Software Reliability.

**Drs. Paul J. Fortier, Hong Liu, Philip H. Viall, and Liudong Xing** are professors of Electrical and Computer Engineering, who have collaborated in security research over the years.

**Dr. Haiping Xu.** Associate Professor of Computer and Information Science, was awarded an NSF grant to investigate an agent-based approach for dynamic trust management in online auctions. The approach ensures the trustworthiness of such systems with real-time monitoring, analyzing, and detection of abnormal bidding behaviors in online auction. He served as a Co-Chair for Software Assurance Session, 26th International Conference on Software Engineering and Knowledge Engineering (SEKE) 2014, and Program Chair for SEKE 2015.

**Dr. Gaurav Khanna.** Associate Professor of Physics, and **Glenn Volkema,** computer technician, recently built a novel supercomputer using consumer video-gaming components over a hundred Sony PlayStations and multiple AMD Radeon graphics-cards. The supercomputer has enabled UMass Dartmouth rank to soar at the absolute top of the RC5-72 contest participant list. This unique system is generating approximately 50 billion keys per second and is slated to have a 1 in 10 chance for winning the contest all by itself.

**Dr. Tien-Shih Hsieh.** Assistant Professor of Accounting and Finance, is interested in researching the impact of regulations on corporate reporting activities and the impact of CEO personal characteristics on business reporting processes. His recent research projects include quantification of the impact of data loss incidents on publically-traded organizations, jointly with Drs. Lance Fiondella and Hong Liu.

**Dr. Timothy Shea.** Associate Professor of Management Information Systems, has focused his research on implementation issues around ERPs, end-user training, Ecommerce, the delivery and management of web-based learning and teaching technologies, and corporate
computer security. He has 18 journal articles published, 7 book chapters, 4 training manuals, and over 50 conference presentations.

**Dr. Adam J. Sulkowski**, Associate Professor of Business Law, specializes in sustainable business, corporate social responsibility, triple bottom line reporting, integrated reporting, and corporate and environmental law. Most notably, he won UMass Dartmouth’s Advisor of the Year Award in 2008 and Holmes-Cardozo Distinguished Paper Award at 2008 Annual Conference of Legal Studies in Business. **Drs. Shea and Sulkowski's** research led to an article on “Cyber-Extortion: The Elephant in the Server Room” in 2007 Journal of Law, Technology & Policy and a chapter on “Cyber Harassment: Strategic Solutions” by Amicus Books 2008.
Appendix III. Lowell: Research Activities

We list the research fields iSAFER members focus on below. The areas are adopted from the core area list compiled by National Centers of Academic Excellence in Information Assurance /Cyber Defense (IA/CD).

1. Security Mechanisms / Functionality
- Cryptography, Identification and Authentication, Authorization and Access Controls
  - Jie Wang, Xinwen Fu
- Wireless, link, and signal security, Virtualization, Audit, monitoring, anomaly detection, DLP (Data Loss Prevention)
  - Xinwen Fu, Benyuan Liu, Guanling Chen, Tricia Chigan

2. Architectures
- Network models, Cloud, Grid, distributed computing, Custom/specialized architectures (e.g. Ad-Hoc Networks), Interconnectivity and routing
  - Jie Wang, Yan Luo, Benyuan Liu, Xinwen Fu, Guanling Chen
- OS/DBMS/Network subjects and objects (active entities and data containers)
  - Cindy Chen, Tingjian Ge
- Critical infrastructure security
  - Xinwen Fu, Tricia Chigan, Ioannis Raptis

3. Assurance
- Testing (functional, penetration, black box, white box, measurement, etc.)
  - Xinwen Fu, Yan Luo, Jie Wang

4. Operations
- Configuration, Security automation, Intrusion detection/analysis/remediation
  - Xinwen Fu, Jie Wang

5. Analysis
- Data mining
  - Cindy Chen, Tingjian Ge, Benyuan Liu, Yu Cao
- Malware analysis, Forensics
  - Xinwen Fu, Jie Wang

6. Non-technical IA Issues
- Legal issues, Policy issues, Privacy, Awareness
  - Xinwen Fu