PROPOSAL FOR

NEW INSTRUCTIONAL PROGRAM

UNIVERSITY OF MARYLAND AT COLLEGE PARK, MARYLAND

PROFESSIONAL STUDIES CERTIFICATE IN CYBERSECURITY LEADERSHIP

ROBERT H. SMITH SCHOOL OF BUSINESS

DEAN G. "ANAND" ANANDLINGAM
# Table of Contents

Executive Summary ................................................................. Page 2  
Purpose of Program ................................................................. Page 2  
Target Audience & Market ......................................................... Page 3  
Collaboration between the Smith, Clark and Public Policy Schools ................. Page 4  
Program Faculty ................................................................. Page 5  
Technical Support Costs ......................................................... Page 5  
Reimbursement for Public Policy and Engineering ..................................... Page 5  
Student Learning Outcomes & Assessments ..................................... Page 5  
Security Needs ................................................................. Page 5  
Original Proposal ................................................................. Page 7  
Appendix A ........................................................................ Page 19  
Appendix B ........................................................................ Page 37  
Appendix C ........................................................................ Page 39  
Appendix D ........................................................................ Page 41  
Appendix E ........................................................................ Page 44  
Appendix F ........................................................................ Page 60  
Appendix G ........................................................................ Page 64  
Appendix H ........................................................................ Page 69  
Appendix I ........................................................................ Page 73
Executive Summary

This summary supports our original proposal, first reviewed on March 27, 2012. Below, we have provided brief answers to the questions raised by the PCC. We have updated and augmented our appendices to provide more detailed information in support of our proposal. The original proposal remains unchanged, other than updates to the admissions language on pages 11 and 16, and to the technology costs in the budget table on page 18.

Purpose of Program

A. Objective: A graduate professional studies certificate program from the University of Maryland in Cybersecurity Leadership launched in partnership between The Robert H. Smith School of Business, The School of Public Policy and the A. James Clark School of Engineering.

Mission: Create a sustainable platform to educate cyber and physical security, supply chain, and acquisition professionals from both government and industry to address leadership skills in this critical national security imperative.

Securing the cyber enterprise and its global supply chain has become a national strategic priority. The President’s Comprehensive National Cybersecurity Initiative (CNCI) and the White House’s National Strategy for Supply Chain Security (released in January 2012) have been two of the most recent and important policy directives addressing this urgent task. These directives provide a compelling rationale for the need for strong multidisciplinary leadership in the cyber enterprise of today and underscore the importance of this new Cybersecurity Leadership Certificate Program.

It is a time of inflection for the cybersecurity profession. The impacts of cybersecurity have reached far beyond the technical community to transform the operating rules of economic competitiveness, diplomacy, and even military conflict.

Government and the private sector increasingly require a new kind of leader who can operate in cyberspace on a planetary scale and help guide border-spanning Information Communications Technology (ICT) ecosystems through the unprecedented challenges of transnational terrorism, commercial espionage, natural disasters, and extreme supply chain disruption. This new type of cyber leader must not only be passionate and technically sophisticated, but must also possess the most up to date enterprise risk management and systems-thinking skills.

The Smith School – with support from a grant from SAIC – has partnered with the A. James Clark School of Engineering and the School Of Public Policy to create a truly unique Certificate Program that fuses the policy, acquisition, supply chain risk management, network security, and innovation and cultural change disciplines to provide students with a solid foundation from a practitioner perspective. We are confident our graduates will be in the vanguard of the profession; well prepared to assume executive roles and craft safer, more secure cyber enterprises.

The content of the five courses that comprise the Certificate in Cybersecurity Leadership encompass Systems Thinking and Design; Cybersecurity Technology; ICT Supply Chain Risk Management, Federal IT
Acquisitions and a highly practical capstone. Course descriptions, including learning objectives and details of assessments may be found in Appendix A. The course content draws on the strengths of the Clark faculty for Cybersecurity Technology and the Capstone, and on Public Policy faculty for Federal IT Acquisition. The Smith School provides content on Systems Thinking and Design and Supply Chain, drawing on original research and award-winning faculty. (See Appendix H for Faculty Bios) The content will be further enhanced by occasional sessions on topics including Leadership communications, innovation, negotiation/partnering, collaboration and strategic thinking, provided by top-ranked Management and Leadership faculty from the business school. The aim of the course is to complement more technical offerings from the Clark school, offering early and mid-career cyber specialists an education in the business of cybersecurity and helping them to further their ambition to become enterprise-wide leaders.

**Target Audience and Target Market**

The Certificate in Cybersecurity Leadership is targeted at early-career and mid-career cyber specialists with titles including Information Security Assessor, Digital Forensics Incident Response Analyst, Systems Operations and Maintenance Professional and Network Security Specialist. These people are likely to be 5-10 years out of college and aged between 28 and 40. They must have 3-5 years of relevant career experience. Smith and Clark have lists of several thousand such professionals working in the Cyber Maryland region, particularly at Aberdeen Proving Ground, Fort Meade/US CyberCommand, Patuxent Air Naval Station and in the DHS and at the Pentagon. Additionally, our excellent alumni and learning and development contacts give us access to professionals and human capital decision-makers within the area’s big defense contractor community. SAIC has offered to promote the program to its contacts and academic co-director, SAIC CTO, Hart Rossman, has facilitated access to the Security Innovation Network and the Governors Workforce Investment Board. Recent interest in the program has come from employees at the Bureau of Alcohol, Tobacco and Firearms, Harris Corporation, Raytheon and the U.S. Army. More data on the current and anticipated growth in the cyber sector in the DC/MD/VA may be found in Appendix E. This document is an abridged version of market research originally compiled by Academic co-Director Dr. Sandor Boyson as part of market research for the program.
Collaboration between the Smith, Clark and Public Policy Schools at University of Maryland, College Park

Governor O’Malley is positioning our state as Cyber Maryland—the world capital of cybersecurity innovation. It is fitting that the state’s flagship University should be a provider of first-rate research and teaching support to our local cyber community. The Certificate in Cybersecurity Leadership, championed by the Smith School, complements existing highly technical initiatives led by the Clark School at College Park, allowing cyber specialists to develop business and leadership skills to supplement their technical expertise. We will teach the business of cybersecurity. We believe that the quality offered by faculty from our three College Park schools allows UMDCP to offer a quality and breadth of education in this area that is unrivaled across the state’s network of universities, and indeed across the world.

We have signed MOUs with both the School of Public Policy and the A. James Clark School of Engineering and have worked closely with Dean Kettl and Dean Pines and their teams to develop and plan to deliver this program. The signed MOUS may be found in Appendix F and Appendix G.

Program Faculty*

<table>
<thead>
<tr>
<th>Cybersecurity Leadership Orientation Bootcamp</th>
<th>Dr. Sandor Boyson &amp; Hart Rossman, SAIC CTO</th>
</tr>
</thead>
</table>

*
| Systems Thinking and Design                  | Dr. Joseph Bailey          |
| Cybersecurity Technology                   | Dr. Michel Cukier          |
| ICT Supply Chain Risk Management           | Dr. Sandor Boyson          |
| Information Technology Acquisition in the Federal Government | Dr. William Lucyshyn & Dan Reddy, CTO EMC |
| Cybersecurity Capstone                     | Dr. Min Wu                |

Full faculty Bios may be found in Appendix H. Additionally, members of Smith’s Management and Organization faculty will teach occasional 90 minute modules, helping students hone their leadership, communications, change management, partnering/negotiation, collaborative, and innovation management skills.

*All program faculty will be members of the University Graduate Faculty.

**Technical Support Costs**

In launch year FY13, it is anticipated that sessions will be largely synchronous with faculty in College Park and students choosing the virtual hub (SMHEC at Patuxent Naval Air Station MD, HEAT at Aberdeen, MD and the Smith Suite at Reagan, DC) most convenient to them for Cybersecurity Technology, ICT Supply Chain Risk Management, and Federal IT Acquisition. The Bootcamp and Capstone will take place at College Park. Students will also complete virtual teamwork utilizing a range of applications currently in everyday use at Smith.

Smith’s Director of IT has produced a detailed breakdown of technology options and the manpower and capital investment needed to support them. This may be found in Appendix I and also within the expenditure table, technology line on page 18. We have costed 21 students (7 at each hub) and have also put in the capital investment costs should the cohort exceed 25 or require an additional hub. Further, we have costed applications allowing student’s personal, remote access to College Park sessions, and applications supporting asynchronous and collaborative work. This provides faculty with more pedagogical flexibility; produces additional options for back-up content delivery should we experience a network outage on days scheduled for synchronous teaching; and allows experimentation and skills-building to inform program delivery in FY 14 and beyond.

**Reimbursement for Public Policy and Engineering**

In line with the MOU’s (Appendices F and G), Smith will pay Clark $752 per student per credit, minus 10% off-campus tuition University overload. Smith will pay Public Policy $661 per student per credit.

**Security Needs: Sensitive Content, Student Identity, and Export Control**

Smith IT will ensure that all technologies are compliant with UMDCP security standards. The students in this program, by its nature, will be much more than averagely aware of cybersecurity and federal compliance issues. Smith will ensure that participants sign an agreement on best practices, and will highlight the Export Control issue with embargoed countries at the College Park bootcamp.
The bootcamp and capstone will be delivered at College Park and virtual, synchronous sessions will be supported by two-way audio visual streaming. The academic co-directors will therefore know the people in the cohort, and can see if they are in class. The requirement to attend class and to be present in College Park makes it unlikely that any student will be from beyond the DC/MD/VA area. Smith is cogniscent of the issues of providing distance learning to out of state or non-US-based students.

Smith will replicate existing proctoring arrangements between Clark and HEAT and SMHEC for exams conducted at the hubs. Smith will follow University protocols for the administration of take home exams.

**Student Learning Outcomes and Assessments**

Within Appendix A we have highlighted the learning objectives and assessment methods and percentages for each for-credit course. The bootcamp is not for credit.

The content for Systems Thinking and Design, and ICT Supply Chain Risk Management is largely based on original research and rigorous instruction and assessment delivered within existing Smith graduate programs. Similarly, Cybersecurity Technology content is currently part of the graduate curriculum at Clark and Federal IT Acquisition is part of a graduate track within the School of Public Policy.
Original Proposal

KIND OF DEGREE: GRADUATE PROFESSIONAL STUDIES CERTIFICATE

Award to Be Offered Proposed initiation Date: August 18, 2012

I. OVERVIEW and RATIONALE

A. Objective: A graduate professional studies certificate program from the University of Maryland in Cybersecurity Leadership launched in partnership between The Robert H. Smith School of Business, The School of Public Policy and the A. James Clark School of Engineering.

Mission: Create a sustainable platform to educate cyber and physical security, supply chain, and acquisition professionals from both government and industry to address leadership skills in this critical national security imperative.

Background: The Supply Chain Management Center faculty at the Robert H. Smith School of Business has been working with SAIC to jointly develop a reference model for Cybersecurity Assurance over the past several years. The reference model presented in 2009 has been recognized in the DoD’s IT Supply Chain state-of-the-art report in August 2010 as a leading reference model. In addition, Dr. Sandor Boyson of the Smith School and Hart Rossman, CTO for Cyber Security Solutions at SAIC, are working with NIST on a project to further define the standards of protecting assets from cyber-attacks on supply chains. Discussions with the University of Maryland’s MC² have brought faculty from the School of Public Policy and the A. James Clark School of Engineering together to provide a unique cross-UMD offering for current and future leaders in government and business.

Market forces: Leading government organizations such as DHS, NSA, GSA, and the DoD are assigning Cybersecurity program management offices (PMOs) with significant support staff that coordinate with smaller staff elements in the line organizations and across the SDLC (acquisition, program management, operations, etc.). This is resulting in new Cybersecurity assurance PMOs for mission-oriented organizations like the Armed Services. In industry, there are an increased number of projects established by large multinational corporations, with an eye towards creating larger Cybersecurity risk management programs.

Governor Martin O’Malley and the Department of Business and Economic Development in Maryland have a Cyber Maryland initiative, designed to promote the state as the world leader in cyber security technology and strategy. Fort Meade MD is the home to U.S. Cyber Command.

At the federal level, there is currently Cybersecurity legislation in the House and Senate. This is the likely next wave of defense and financial spending and regulation post Iraq/Afghanistan and TARP.
B. The target enrollment - how big is the program expected to be? From what other programs serving current students, or from what new populations of potential students, onsite or offsite, are you expecting to draw?

For the inaugural cohort we expect a class of 20 information technology professionals with a BS in computer science, electrical engineering or information systems in one of the job titles identified by the NICE Initiative. These prospective students may want to get an MS degree and seek a gateway program that can help them explore and jumpstart either an advanced technical or management career option. We will also target Public Policy graduates with a federal acquisition tract, US Cyber command in Ft. Meade, and high tech defense contractors.

The combined focus on leadership and technical expertise is a differentiator, allowing us to compete with other institutions that may be focused solely on the basics on the basics of Cybersecurity, or the technical certifications.

Top commercial targets: banks, utilities, credit card companies in DE (close to a proposed virtual learning location at Aberdeen MD), companies in IT support roles for the US and state governments across the region.

Top federal targets: DHS, DOD, NSA, FBI, CIA, DHHS

We anticipate students will be drawn from a wide geographic area centered on the Washington region and will not be limited to individuals working or living in the College Park area.

II. CURRICULUM

A. Provide a full catalog description of the proposed program, including educational objectives and any areas of concentration.

Professional Studies Cybersecurity Leadership Certificate Program - The program provides an advanced educational foundation for Cybersecurity professionals and managers who have already exhibited strong career accomplishments. Program prerequisites include a bachelor’s degree and professional or managerial work experience beyond the bachelor’s degree. This would typically amount to a minimum of 3-5 years. The program requires 15 credits of coursework over a 4-month period. Successful students in the program are expected to demonstrate thorough and integrated knowledge of (1) the tools, concepts and theories relating to systems and design thinking, Cybersecurity technology, ICT supply chain risk management, and federal IT acquisition, (2) behavioral and strategic skills necessary to step up to enterprise-wide management or leadership.

After a ‘boot camp’ to kick the program off in College Park, MD, content is delivered in a virtual-hub format, creating ease of access and convenience for participants from three of the following locations: The Ronald Reagan Building in Washington, DC, Aberdeen Proving Ground, Fort Meade, and Patuxent Naval Air Station in Maryland. The program is offered by the Robert H. Smith School of Business and taught by team of faculty from the top-ranked A. James Clark School of Engineering, The Robert H. Smith School of Business and the University of Maryland’s School of Public Policy. Students will also have
access to a “virtual lab’ created specifically for this program, where classmates will work collaboratively on projects and assignments.

B. List the courses (number, title, semester credit hours) that would constitute the requirements and other components of the proposed program. Provide a catalog description for any courses that will be newly developed or substantially modified for the program.

Proposed Curriculum:

15 credits, 5 courses, each course 3 credits = 37.5 credit hours per course
*Boot Camp is considered an advanced orientation that is mandatory and does not offer credit

<table>
<thead>
<tr>
<th>Course</th>
<th>Course Number</th>
<th>Faculty Leader</th>
<th>Catalog Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity Leadership Boot Camp*</td>
<td></td>
<td>Smith School</td>
<td>The Cybersecurity Leadership Boot camp is an intensive one-day experience that will demonstrate the value of your certificate studies to your career development and enterprise-wide risk management responsibilities. No credit will be earned from taking this course; however, it is required for the certificate.</td>
</tr>
<tr>
<td>Systems &amp; Design Thinking</td>
<td>BULM 758L</td>
<td>Smith School</td>
<td>This course will use a systems thinking approach to understand issues related Cybersecurity. We begin by understanding what the systems thinking approach is and why it is valuable when addressing problems that are inherently complex. Specifically, systems and design thinking enables a manager to anticipate the direct and indirect consequences of an action so that they can use an approach that holistically solves complex problems instead of portions of them.</td>
</tr>
<tr>
<td>Government IT Acquisitions &amp; Contracting Considerations</td>
<td>PUAF 689F</td>
<td>Public Policy</td>
<td>This course provides an overview of acquisition as one of the basic functions of government, all aspects of federal government contracting, subcontracting and related challenges,</td>
</tr>
<tr>
<td>Course</td>
<td>Code</td>
<td>School</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>---------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Acquisition track Masters in Public Policy)</td>
<td></td>
<td></td>
<td>From the development of solicitation to final close-out, within the context of the federal laws and the Federal Acquisition Regulations (FAR), and explore ways to improve (from a public policy perspective) the efficiency and effectiveness with which the government goes about acquiring well over $300 Billion of goods and services.</td>
</tr>
<tr>
<td>Cybersecurity Technology</td>
<td>ENRE 684</td>
<td>Clark School</td>
<td>The course will discuss the main concepts of Cybersecurity, how to manage Cybersecurity, the main security models and how to evaluate Cybersecurity. The course will also review how security is implemented in operating systems (Unix and Windows), databases, software, networks, web, and mobile devices.</td>
</tr>
<tr>
<td>ICT Supply Chain Risk Management (Core Curriculum for the Masters in Supply Chain)</td>
<td>BULM 744</td>
<td>Smith School</td>
<td>This course explores methods to build ICT Supply Chain Risk Management (SCRM) capability from multiple perspectives:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-From the perspective of the cyber supply chain planner who has to assess strategic &amp; operational ICT risks on a system-wide basis.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-From the perspective of the cyber supply chain operations director who must help ensure that enterprise ICT systems adapt to day-to-day uncertainties.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-From the perspective of cyber supply chain customers who are concerned about how to ensure day to day business continuity of ICT systems and also cope with low probability but high impact events such as a cyber-terrorist event.</td>
</tr>
<tr>
<td>Capstone – Cybersecurity Leadership</td>
<td>BULM 758P</td>
<td>Collective</td>
<td>This capstone course on Cybersecurity Leadership builds on the background from other foundational courses in the</td>
</tr>
</tbody>
</table>
Professional Studies Cybersecurity Leadership Certificate program and utilizes team-based consulting projects to provide students with a methodology and hands-on experiment for diagnosing and solving real world Cybersecurity assurance problems.

For complete course descriptions, please see Appendix A.

C. Describe any selective admissions policy or special criteria for students selecting this field of study.

Admission to the Certificate program is highly competitive and is based on significant and relevant professional and managerial work experience and prior academic performance. Each applicant is considered on a case-by-case basis. The admissions requirements for the program reflect the standards upheld by the University's Graduate School.

Applicants will have earned a bachelor’s degree at a regionally accredited college or university in the United States, or the equivalent in another country. Applicants’ transcripts should reflect a minimum standard of a 3.0 average in all undergraduate courses taken. Applicants who received their bachelor’s degree from a foreign university may have to demonstrate English proficiency.

III. STUDENT LEARNING OUTCOMES AND ASSESSMENT

A. List the program’s learning outcomes and explain how they will be measured.

Systems Thinking – Learning outcomes will be assessed through the administration of a mid-term (See Appendix B) and final examination

- Recognize when a systems approach would be the appropriate course of action instead of a traditional or linear approach.
- Use the systems thinking process to address a problem or opportunity in developing a solution.
• Develop a model that best approximates the systems solution in order to understand the direct and indirect effects of a solution.

• Communicate the systems solution effectively to a diverse audience including those not familiar with the systems approach.

• Develop a strategic plan consistent with the systems approach that will minimize exposure to risk and allow for risk mitigation and contingency planning.

• Understand the systems approach in the context of a Cybersecurity in planning and building secure networks.

*Cybersecurity Technology* - Learning outcomes will be assessed through the administration of a mid-term and final exam

• Recognize the significance of Cybersecurity.

• Define approaches for securing various aspects of the cyber supply chain: the hardware, software and human level.

• Explore a particular aspect of the cyber supply chain and discuss how to secure it.

*ICT Supply Chain Risk Management* - Learning outcomes will be assessed through the administration of a graded team-based computer industry simulation

• Gain grounding in the foundational concepts and techniques for supply chain risk management.

• Explore the risks of counterfeits, malware and state-sponsored or criminal intrusions and best practices for managing these risks.

• Consider how to assure defense in depth in all phases of the systems development lifecycle and to manage defense in breadth across the operations of extended supply chains.

• Use two industry-leading risk models: the Supply Chain Council’ supply chain operations reference model (SCOR) and the Council of Supply Chain Management Professional’s X-Treme Supply Chain Management model and learn how SCRM concepts and techniques are being applied to the ICT supply chain.

*Information Technology Acquisition in the Federal Government* - Learning outcomes will be assessed by requiring students to write three short (four pages max.) “issue papers” based on a topical IT acquisition issue and a final exam

• Describe the federal acquisition environment, along with its regulations and processes.

• List key challenges typically encountered during the contracting for and while managing IT projects.
• Articulate the primary threats to government cyber systems

• Differentiate between compliance that COTS vendors undertake for compliance versus risk management undertaken by the acquiring agency

Cybersecurity Leadership Capstone - Learning outcomes will be assessed through the administration of at least 2 graded team-based transformational projects

• Detail the significance of Cyber Supply Chain Assurance in today’s business operations.

• Outline Cyber Supply Chain Assurance practices, including analyzing threats, defining reasonable assurance objectives, identifying potential solutions, and assessing the technical, business, and social cost-benefits of candidate solutions.

• Gain heightened exposure to the complexity of assurance issues and decisions related to cyber supply chain management to critical client groups and emerging markets.

B. Include a general assessment plan for the learning outcomes. (In lieu of a narrative for both IIIA and IIIB, you may attach the program’s learning outcomes assessment forms.)

Students will be assessed at the conclusion of each course on the aforementioned learning outcomes. Feedback gathered will be used to continuously improve the program for future cohorts. Students will also be given a comprehensive assessment of the entire program upon completion.

IV. FACULTY AND ORGANIZATION

A. Who will provide academic direction and oversight for the program?

Oversight of the program will be provided by the Office of Executive Programs at the Smith School of Business. In the Office of Executive Programs at the University of Maryland’s Robert H. Smith School of Business, we provide adult learning experiences that span the spectrum of time and customization. Academic direction for the CSLC program will be provided by the joint Academic Directors appointed by the Assistant Dean of the Office of Executive Programs, Dr. Sandor Boyson, Director Supply Chain Management Center at Smith and Hart Rossman, CTO, SAIC.

B. If the program is not to be housed and administered within a single academic unit, provide details of its administrative structure. This should include at least the following:

i. Participating units.

While the Professional Studies Cybersecurity Leadership Certificate is taught in partnership between the Robert H. Smith School of Business, The A. James Clark School of Engineering, and The School of Public Policy, the Office of Executive Programs will be providing all administration and oversight of the program, which will be offered through Smith.

ii. Academic home and reporting relationship of the program director.
The Robert H. Smith School of Business is the academic home and its Senior Director for Executive Custom Programs is the program director.

iii. Composition and authority of a faculty oversight committee.

CSLC policy and curricular issues will be decided with the guidance and approval of the CSLC Oversight Committee composed of Senior Director of Executive Custom Programs, and the Academic Director. The Oversight Committee advises the Assistant Dean for Executive Programs on all matters of academic policy and curriculum, and participates directly in the selection of courses for each entering cohort.

iv. Process for assigning faculty to needed courses, and agreements with departments for releasing faculty or for allowing faculty overload for this purpose. Source for teaching assistants, if needed.

Faculty will be selected to teach in the program by the Oversight Committee in consultation with the Assistant Dean of Executive Program and the respective Department Chairs in the respective Schools. Staffing will be accomplished on an overload basis. We do not anticipate the need for teaching assistants.

v. Arrangements for student advisement. For a graduate program, arrangements for research mentoring, assistantships, laboratory access, access to other resources, etc., as applicable.

As a professional certificate program delivered either on-campus or off-campus there will not be a need for additional on-campus research facilities or support. Students will require access to campus computer accounts, but no other support resources other than this will be required. We anticipate the large majority of students will be employed full-time and so not in need of career guidance or placement advising beyond that available via normal faculty interaction.

vi. Process for recommending and proposing program changes. Process and schedule for program review.

The CSLC Oversight committee will review and make recommendations for program changes in consultation with the Assistant Dean for Executive Programs and the Dean’s Office. Full program reviews will be conducted at least once every year.

V. OFF CAMPUS PROGRAMS

A. If the program is to be offered to students at an off-campus location, with instructors in classrooms and/or via distance education modalities, indicate how student access to the full range of services (including advising, financial aid, and career services) and facilities (including library and information facilities, and computer and laboratory facilities if needed) will be assured.

The program will be offered in real time and will consist of one-eighteen week term. We plan to broadcast the program to multiple locations in a virtual synchronous format, allowing local learning, live peer support and virtual convenience. This is a model widely used by the Clark School of Engineering and utilizes our Telepresence facilities within Smith, and builds on existing UMD CP relationships with
higher education institutions close to Patuxent Naval Air Station and Fort Meade, MD. We also plan to offer students the opportunity to learn within the Smith School of Business classrooms at the Ronald Reagan Building in Washington D.C., and at Aberdeen Proving Ground where they have classrooms supporting live streaming facilities. Students will be provided with all relevant class materials electronically. Adequate computer lab facilities already exist in all locations and the nature of the student body precludes any need for campus-based financial aid or career services.

B. If the program is to be offered mostly or completely via distance education, you must describe in detail how the concerns in Principles and Guidelines for Online Programs are to be addressed.

To assure academic quality, all online programs will adhere to the policies and concerns outlined in the University of Maryland document, Principles and Guidelines for Online Programs.

Program Initiation and Choice - The proposal was initiated within the Office of Executive Programs and has the approval of Dean G. “Anand” Anandalingam. This proposal was developed as a result of the school strengths and aligns with the schools strategic goals (See Appendix C).

Program Development, Control and Implementation by Faculty - The faculty will have overall control over the design, development, and will have the overall bulk of the academic instruction. Smith school technical support personnel will be available, as well as agreements with the off-campus sites for technical support during classroom hours. Support will be available to faculty during course development, as well as during the offering of the program.

Access to Academic Resources and Student Services - Student services such as admissions, registration, bill payment, advisement, and bookstore services will be facilitated through the Office of Executive Programs. Library services will be available through Virtual Business Information Center (VBIC).

Intellectual Property Rights – None required

Full Disclosure, Standards, and Evaluation - All published materials describing the program will carefully lay out instructional methods to be used, the skills and background necessary for success, academic support and resources, and available student services. Potential candidates will be given the opportunity to complete the Certificate Admissions Questions document (See Appendix D) prior to applying to the program. This document will be posted on the program website and potential candidates will submit the document to the Academic Director prior to them applying to the program. The Academic Director will advise the candidate of their readiness to apply to the program based on their responses. Academic admission standards will be clearly described, and will be consistent with those for on-campus programs. Every year the Oversight committee will evaluate the program to ensure all standards are being met.

VI. OTHER ISSUES

A. Describe any cooperative arrangements with other institutions or organizations that will be important for the success of this program.
For this program, The Smith School of Business has a standing MOU with SAIC to provide financial and physical assets (virtual lab). In addition, we have agreements with the A. James Clark School of Engineering and the School of Public Policy to jointly promote and cooperate to build a powerful and impactful program for mutual benefit. All other arrangements (virtual hubs) will be made under either vendor-based agreements with third-parties (e.g., HEAT center in Aberdeen), or MOU’s that provide access to learning facilities that would benefit employees of that entity (e.g., DoD at Ft. Meade).

B. Will the program require or seek accreditation? Is it intended to provide certification or licensure for its graduates? Are there academic or administrative constraints as a consequence?

No accreditation is needed or sought. Graduates will not be seeking licensure or certification of any kind.

VII. COMMITMENT TO DIVERSITY

Identify specific actions and strategies that will be utilized to recruit and retain a diverse student body.

Admissions processes will reflect the requirements outlined for a non-degree seeking student to the graduate school, as outlined on pg. 11 and so afford all of the opportunities for diversity as now exist with those programs.

VIII. REQUIRED PHYSICAL RESOURCES

A. Additional library and other information resources required to support the proposed program. You must include a formal evaluation by Library staff.

None required

B. Additional facilities, facility modifications, and equipment that will be required. This is to include faculty and staff office space, laboratories, special classrooms, computers, etc.

None required

C. Impact, if any, on the use of existing facilities and equipment. Examples are laboratories, computer labs, specially equipped classrooms, and access to computer servers.

No impact on existing facilities beyond those that are already in place is anticipated.

IX. RESOURCE NEEDS and SOURCES

Describe the resources that are required to offer this program, and the source of these resources. Project this for five years. In particular:

A. List new courses to be taught, and needed additional sections of existing courses. Describe the anticipated advising and administrative loads. Indicate the personnel resources (faculty, staff, and teaching assistants) that will be needed to cover all these responsibilities.
For the first cohort, one new section of the courses listed in section II, B, ii will be required. These will be staffed on an overload basis out of tuition revenue. The same will be true of the orientation/boot camp. This mode of staffing and funding will continue until such time as stabilized demand is observed and hiring to enable on-load delivery then initiated. No additional staff beyond the administrative program manager is anticipated.

B. List new faculty, staff, and teaching assistants needed for the responsibilities in A, and indicate the source of the resources for hiring them.

With initial program delivery taking place via overload instruction, no hiring will be required in year one. Hiring to support program growth and conversion to on-load delivery may be necessary in years 3-6 following program launch.

C. Some of these teaching, advising, and administrative duties may be covered by existing faculty and staff. Describe your expectations for this, and indicate how the current duties of these individuals will be covered, and the source of any needed resources.

Via overload as described above

D. Identify the source to pay for the required physical resources identified in Section VIII. above.

None required

E. List any other required resources and the anticipated source for them.

None required

F. Provide the information requested in Table 1 and Table 2 (for Academic Affairs to include in the external proposal submitted to USM and MHEC).

<table>
<thead>
<tr>
<th>MHEC TABLE 1: RESOURCES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resources Categories</strong></td>
</tr>
<tr>
<td>1. Reallocated Funds</td>
</tr>
<tr>
<td>2. Tuition/Fee Revenue</td>
</tr>
<tr>
<td>a. # FT Students</td>
</tr>
<tr>
<td>b. Annual Tuition/Rate</td>
</tr>
<tr>
<td>c. Annual Full Time</td>
</tr>
<tr>
<td>d. # Part Time Students</td>
</tr>
<tr>
<td>e. Credit Hour Rate</td>
</tr>
<tr>
<td>f. Annual Credit Hours</td>
</tr>
<tr>
<td>g. Total Part Time</td>
</tr>
<tr>
<td>3. Grants, Contracts, &amp;</td>
</tr>
<tr>
<td>Other External Sources</td>
</tr>
<tr>
<td>TOTAL (Add 1 – 4)</td>
</tr>
</tbody>
</table>
*Credit Hour Rate subject to change with Part-time MBA program Credit Hour Rate adjustments.

**Stipend received from Science Application International Corporation (SAIC) to pay faculty to develop content from the program and to assist with marketing. Going forward, the revenue generated from the program will cover these costs.

<table>
<thead>
<tr>
<th>MHEC TABLE 2: EXPENDITURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expenditure Categories</td>
</tr>
<tr>
<td>----------------------------</td>
</tr>
<tr>
<td>1. Total Faculty Expenses (b + c below)</td>
</tr>
<tr>
<td>a. # FTE</td>
</tr>
<tr>
<td>b. Total Salary</td>
</tr>
<tr>
<td>c. Total Benefits*</td>
</tr>
<tr>
<td>2. Total Administrative Staff Expenses (b + c below)</td>
</tr>
<tr>
<td>a. # FTE</td>
</tr>
<tr>
<td>b. Total Salary</td>
</tr>
<tr>
<td>c. Total Benefits</td>
</tr>
<tr>
<td>3. Total Support Staff Expenses (b + c below)</td>
</tr>
<tr>
<td>a. # FTE</td>
</tr>
<tr>
<td>b. Total Salary</td>
</tr>
<tr>
<td>c. Total Benefits</td>
</tr>
<tr>
<td>4. Equipment</td>
</tr>
<tr>
<td>5. Clark/PubPol Reimbursement</td>
</tr>
<tr>
<td>6. New or Renovated Space</td>
</tr>
<tr>
<td>7. Technology Expenses**</td>
</tr>
<tr>
<td>TOTAL (Add 1 – 7)</td>
</tr>
</tbody>
</table>

*Faculty will be paid on an overload basis. Benefits will still be paid through their department home.

**Please see Appendix I for detailed break down of technology expenses.
Cybersecurity Leadership Boot Camp:

The Cybersecurity Leadership Boot camp is an intensive one-day experience that will demonstrate the value of your certificate studies to your career development and enterprise-wide risk management responsibilities. No credit will be earned from taking this course; however, it is required for the certificate.

Hart Rossman, SAIC VP and Chief Technology Officer Cyber Programs (Co-Academic Director) shares an overview of the opportunities and imperatives in the fast-growing Cybersecurity job market. His central message: Global businesses and national governments need the skills you will develop this semester.

Benefit from Leadership faculty support to begin work on your personal career development plan, considering the behaviors you wish to enhance, adopt or let go as you make the move from functional expert to organization-wide leader, or to Cybersecurity change-maker.

Explore two development paths:

Nine credits from your certificate studies may be applied to the following Masters of Science degrees from the University of Maryland, College Park.

- **MS Cybersecurity Engineering from the A. James Clark School of Engineering**
  --ideal for subject matter experts who wish to lead through research-based innovation
- **MS Information Systems from the Robert H. Smith School of Business**
  --ideal for ambitious managers who seek enterprise-wide, strategic leadership roles.

Academic Co-Director Dr. Sandor Boyson will help you drive the most value from:

- your relationship with the University of Maryland, College Park
- certificate faculty, experts and materials
- and the peer network you will access in your chosen classroom and via our virtual learning hub.

The bootcamp will conclude with a private dinner offering an opportunity for you to get to know the cohort—a valuable network which can support you during your studies and long into your future.

**BULM 758L - Systems & Design Thinking:**

Course Description

This course will use a systems thinking approach to understand issues related to design in the cybersecurity context. We begin by understanding what the systems thinking approach is and why it is
valuable when addressing problems that are inherently complex. Specifically, systems thinking enables a manager to anticipate the direct and indirect consequences of an action so that they can use an approach that holistically solves complex problems instead of portions of them. In this class, we will examine systems that may appear to be serial in nature but have some feedback loops when examined from a holistic perspective. Then, we will describe the principles of systems design in order to use positive feedback loops to better manage complex systems by reducing the time to convergence and preventing systems that are chronically “out of control.” This course will take these concepts and explore them in the context of managing complexity in cybersecurity. We will draw on real-world examples of how systems may be sub-optimized if improperly designed or understood. The course will use an iterative approach to teaching that uses three in-depth cases where student teams are asked to design and then improve cybersecurity using the systems approach.

**Learning Objectives**
**After the completion of this course, a student will be able to:**

- Recognize when a systems approach would be the appropriate course of action instead of a traditional or linear approach.
- Use the systems thinking process to address a problem or opportunity in developing a solution.
- Develop a model that best approximates the systems solution in order to understand the direct and indirect effects of a solution.
- Communicate the systems solution effectively to a diverse audience including those not familiar with the systems approach.
- Develop a strategic plan consistent with the systems approach that will minimize exposure to risk and allow for risk mitigation and contingency planning.
- Understand the systems approach in the context of a cybersecurity and how the systems approach may be used in this context.

**Required Materials**
This course will have a course packet containing cases and book chapters pertinent to our course material. This includes chapters from the book:


This course packed will be supplemented during the semester by articles in the news relevant to the course concepts.

**Grading**
**Students in this course will be graded based on a combination of individual and team deliverables. A summary of these deliverables and associated weights are:**

<table>
<thead>
<tr>
<th>Individual deliverables</th>
<th>Team Deliverables</th>
</tr>
</thead>
</table>

20
5% Individual Statement
15% First Exam
15% Second Exam
15% Peer Evaluation

5% Team Charter
The instructor will assign teams on the first day of class. By the end of the first class, each team should submit a team charter that will detail the shared mission of the team and how that team will coordinate among team members throughout the semester. Although the teams will update their charters throughout the semester, this initial document will be graded for completeness.

5% Individual Statement
At the start of the second class, the instructor will collect an individual statement from each student that describes their background and experience with a systems approach to solving problems. This document should be no longer than one page and will serve as a foundation for learning for each student during the semester.

30% (5% x 6) Team Case Presentations
A key component of learning the course material is for students to design and improve systems. Accordingly, there are three cases throughout the semester where teams are allowed to design and improve different systems to address potential cybersecurity risks. For each case, a team will propose their design in one class. In a subsequent class, another team will take that design and improve it.

15% First Exam
Students will have an in-class exam during the 9th session that will test them on concepts covered to that point.

15% Second Exam
There will be a take-home exam after the last class that students should complete using the course web site.

15% Peer Evaluation
At the conclusion of the semester, each student will evaluate themselves and their teammates’ contributions to the team. A simple instrument will be uses whereby students will distribute 100% among their team members and then briefly justify their reasoning. Students receiving consistently low percentages will earn a lower grade for this item.

15% Final Team Presentation
During the 14th class session, teams will make a 30 minute presentation on a technology, business, or market in the cybersecurity industry that can be improved by taking the systems thinking approach. Teams are to describe the context and associated terms within this context. They are then to explain how much (or little) of the status quo uses a systems approach. Then, teams are asked to make recommendations regarding how a system approach would improve the approach. Students are
expected to draw on concepts from the class including building a model to describe their improved system.

On each assignment you will be asked to write out and sign the following pledge. "I pledge on my honor that I have not given or received any unauthorized assistance on this exam/assignment."

Special Administrative Considerations
If you are a student with special learning needs, please let the instructor know via email before the second class so that he can make any appropriate adjustments.

Class Schedule

<table>
<thead>
<tr>
<th>Session</th>
<th>Topics</th>
<th>Deliverables</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Introduction to Systems Thinking</td>
<td>Team Charter</td>
</tr>
<tr>
<td>1.2</td>
<td>Tenants of the Systems Approach</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Stakeholders</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Holistic approach</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Temporal thinking</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Systems Analysis and Design Tools</td>
<td>Individual Statement</td>
</tr>
<tr>
<td></td>
<td>• Interrelationship diagrams</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fishbone diagrams</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Tornado diagrams</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multiattribute utility analysis</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Mitigation and Contingency Planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Direct and indirect effects</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unintended consequences</td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Developing a System Model</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Modeling software to aid in a systems approach</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sensitivity analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Monte Carlo simulation</td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>Systems Design of Case 1: Denial of Service Attack</td>
<td>Team Presentation #1</td>
</tr>
<tr>
<td>3.3</td>
<td>Systems Improvement of Case 1</td>
<td>Team Presentation #2</td>
</tr>
<tr>
<td>3.4</td>
<td>Feedback Loops</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identification of feedback loops within a system</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Designing feedback loops</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fuzzy logic associated with feedback loops</td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Idealized Design</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Systemic design</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Voice of the customer and users</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Event</td>
<td>Notes</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>4.2</td>
<td>Midterm Exam</td>
<td>First Exam</td>
</tr>
<tr>
<td>5.1</td>
<td>System Dynamics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Convergence and Divergence of systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Agility</td>
<td></td>
</tr>
<tr>
<td>5.2</td>
<td>Systems Design of Case 2: Intruder Detection in an Inter-Enterprise IT System</td>
<td>Team Presentation #3</td>
</tr>
<tr>
<td>5.3</td>
<td>Systems Improvement of Case 2</td>
<td>Team Presentation #4</td>
</tr>
<tr>
<td>5.4</td>
<td>Systemic Improvement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Continuous process improvement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cultural changes within and between organizations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transformation of people, processes, and technology</td>
<td></td>
</tr>
<tr>
<td>6.1</td>
<td>Final Team Presentations</td>
<td></td>
</tr>
<tr>
<td>6.2</td>
<td>Systems Designs of Case 3: Semiconductor Supply Disruptions in Upstream Production</td>
<td>Team Presentation #5</td>
</tr>
<tr>
<td>6.3</td>
<td>System Improvement of Case 3</td>
<td>Team Presentation #6</td>
</tr>
<tr>
<td>6.4</td>
<td>Course Recap</td>
<td>Take-Home Second Exam</td>
</tr>
</tbody>
</table>

**ENRE 684 - Cybersecurity Technology:**

**I. Purpose of Course:**

The goal of this course is to provide an introduction to cybersecurity. The course is developed such that no prerequisite is needed to take this course. The course will discuss the main concepts of cybersecurity, how to manage cybersecurity, the main security models and how to evaluate cybersecurity. The course will also review how security is implemented in operating systems (Unix and Windows), databases, software, networks, web, and mobile devices. Security approaches will be classified into prevention, detection and tolerance. Both the defense and the attacker perspectives will be addressed.

**II. Key Course Learning Objectives:**

Students will be able to:

1. Appreciate why cybersecurity is essential to all organizations and describe the risks associated with security gaps or lapses at the brand/reputation, operational, safety or sustainability level.
2. Recognize and describe common and emerging forms of defenses and attacks.
3. Apply learned methods for securing organizations at the hardware, software and human level.

III. Readings:

A. Textbook

IV. Session Plan

Session 1 – Saturday 9/29
Course Introduction
Foundations of Cybersecurity (chap. 3)
Managing Cybersecurity (chap. 2)
Risk Assessment
Identification and Authentication (chap. 4)
Access Control (chap. 5)

Session 2 – Tuesday 10/2
Security Models (chaps. 11 & 12)
Cryptography (chap. 14)
Key Management (chap. 15)

Session 3 – Saturday 10/6
Security Evaluation (chap. 13)
Application: Operating Systems Security (Unix and Windows) (chaps. 7 & 8)
Leading Organizational Change
Midterm
Topics for Students Presentations

Session 4 – Tuesday 10/9
Application: Database Security (chap. 9)
Application: Software Security (chap. 10)
Application: Communication Security (chap. 16)

Session 5 – Saturday 10/13
Application: Network Security (chap. 17)
Application: Web Security (chap. 18)
Application: Mobile Devices Security (chap. 19)
Students Presentations

Session 6 – Tuesday 10/16
Students Presentations
Final Exam
Course Feedback

V. Course Grading:
**Final grades will be determined using the following distribution:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Homework</td>
<td>15%</td>
</tr>
<tr>
<td>Presentation</td>
<td>20%</td>
</tr>
<tr>
<td>Participation</td>
<td>10%</td>
</tr>
<tr>
<td>Midterm</td>
<td>25%</td>
</tr>
<tr>
<td>Final</td>
<td>30%</td>
</tr>
</tbody>
</table>

In addition to lectures, students will select a particular aspect of the cyber supply chain and investigate possible Cybersecurity solutions. Students will present these solutions during class time to discuss them with the other students.

**BULM 744 - ICT Supply Chain Risk Management:**

1. **Introduction**

Securing the Cyber-Supply Chain has become a national strategic priority. The President’s Comprehensive National Cybersecurity (CNCI) Initiative and the White House’s National Strategy For Supply Chain Security (released in January, 2012) have both addressed this urgent task.

Yet our own research at the R.H. Smith School Of Business’ Supply Chain Management Center, conducted in partnership with the National Institute Of Standards And Technology (NIST) has led to one inescapable conclusion: the cyber supply chain today is as fragmented and stove piped today as the physical product supply chain was in the mid-1990s.

In an earlier work, “Toward A Cyber-Supply Chain Code of Practice” (NIST, March 2011), we concluded: “The cyber supply chain risk management discipline is currently in an early emerging state characterized by: a deficient evidence-based body of knowledge; a proliferation and fragmentation of industry best practices and standards groups, generally led by only the largest firms; and a profound under-usage of supply chain-wide risk governance mechanisms inside IT vendors”. (p.45)

In our 2011 survey of over 200 IT Vendors to the federal Enterprise, we found that: "On the strategic side of risk management, 47.6% of our sample of 200 IT companies never uses a Risk Board or other executive mechanisms to govern risk; 46.1% never uses a shared Risk Registry, an online database of IT supply chain risks; 49.4% never uses an integrated IT supply chain risk management dashboard; and 44.9% say they never use a supply chain risk management plan." (ibid, p.20). At the other end of the spectrum, there are coverage gaps at the lowest level of field operations. Many IT companies do not address the need for automated business rules and sensor-driven responses, e.g. they cannot sense and respond to risks in real time.
Currently, there are over sixty industry and public sector Information communications technology (ICT) supply chain risk management Initiatives in software, hardware, network, and system integration services that seek to address the dual challenges of assuring defense in breadth and defense in depth. Defense in breach is extensive: it covers the whole business ecosystem of system acquirers, integrators, suppliers and their key shared processes. Defense in depth is intensive: it covers risk governance; systems lifecycle (SDLC) management (including design, risk assessment and supply base modeling/auditing); and operations management.

This course will orient the student to the critical new discipline of cyber supply chain risk management and to the standards, practices and toolsets that mark this discipline. Our course content fuses together the fields of cyber security, supply chain management and risk analytics to address the quality assurance and business continuity challenges/ opportunities of the cyber supply chain, which is defined by these three main elements:

-Cyber infrastructure: The mass of IT systems (hardware, software, and public/private and classified networks) that, together, constitute the backbone of important national and enterprise infrastructure. This infrastructure enables the uninterrupted operations of key government and industrial base actors such as the Department of Defense, the Department of Homeland Security, and their major suppliers.

-Cyber supply chain: The entire set of key actors involved with/using cyber infrastructure: system end-users, policy makers, acquisition specialists, system integrators, network providers, and software/hardware suppliers. The cyber supply chain is characterized by these users/providers’ organizational and process-level interactions to plan, build, manage, maintain, and defend cyber infrastructure.

-Cyber Supply Chain Assurance Reference Model: A model that not only defines key actors, processes, and vulnerabilities, but also identifies strategic interdependencies at each node of the international production/sustainment chain

We will explore methods to build cyber supply chain resiliency from multiple actor perspectives:

-From the perspective of the cyber supply chain planner who has to assess strategic & operational ICT risks on a system-wide basis.

-From the perspective of the cyber supply chain operations director who must help ensure that enterprise ICT systems adapt to day-to-day uncertainties.
-From the perspective of **cyber supply chain customers** who are concerned about how to ensure day to day business continuity of ICT systems and also cope with low probability but high impact events such as a cyber-terrorist event.

II. Objectives

Cyber Supply Chain Risk Management: Learning Objectives:

1. The student will demonstrate a working knowledge of the fundamental components of the cyber supply chain and be able to utilize standard commercial templates such as those provided by the Supply Chain Council Operations Reference Model (SCOR) to construct a process map of an integrated ICT system composed of hardware, software and network elements.

2. The student will be able to identify the key strategic, industry and company-level forces driving the need for a formal Enterprise Risk Management (ERM) Program; and the historical evolution, organizational structures and implementation roadmaps in use in leading ICT companies through detailed case analyses.

3. The student will be able to use basic risk assessment methodologies such as the use of probability/severity matrixes to assess the frequency and impact of key risks on the cyber supply chain.

4. The student will be able to navigate an advanced risk assessment software tool - @Risk software - and use it to construct a Monte Carlo Exercise capable of running a simple cyber supply chain risk analysis model through a thousand iterations.

5. The student will be able to demonstrate an understanding of industry best practice guidelines and standards (such as NIST’s IT Risk Management Standards or the Open Group’s Trusted Technology Practices) through the production of a Strategic Cyber Supply Chain Risk Management Plan for his/her organization.

III. Required Materials

Assigned Readings:

**Module 1: The Landscape Of Cyber Supply Chain Security**


(csrc.nist.gov/scrm/documents/umd_ict_scrm_initiatives-report2-1.pdf)

Microsoft, “Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust”
Microsoft, “Toward a Trusted Supply Chain: A Risk Based Approach to Managing Software Integrity”


Telcom Carrier Working Group,”Foreign Supply Chain Security Risk Management: A Proposed Model, Protecting the U.S. Public Telecommunications Network Infrastructure”

Global Innovation & Strategy Center, “US Reliance on Foreign IT, Mitigating Risks Associated with Foreign Sources of Hardware Components


Fortune, “The global supply chain: So very fragile” December 12, 2011

Supply Chain Digest “The 11 Greatest Supply Chain Disasters”, 2006


Chopra, Sunil “Managing Risk To Avoid Supply Breakdown”, MIT Sloan Management review fall 2004

Yossi Sheffi; James B. Rice Jr. “Supply Chain View of the Resilient Enterprise “, English PDF | SMR185-PDF-ENG (Harvard Course Pack)**


Norrmam, Andreas, “Ericsson’s proactive supply chain risk management approach after a serious sub-supplier accident”, International Journal Of Physical Distribution &Logistics Management, Vol.34 No.5 2004

Module 2: Cyber Supply Chain Enterprise Risk Management

CIO, “ERM Strategic Guide for CIOs”


NIST, “Risk Management Guide for Information Technology Systems”

NIST, “Contingency Planning Guide for Information Technology Systems”


Miklovic, Dan, “Case Study: CISCO Addresses Supply Chain Risk Management”, Gartner, 2010
Module 3: Cyber Supply Chain Risk Management Tools/Techniques


SafeCode, “Software Integrity Controls”

The Open Group, “Open Trusted Technology Provider Framework (O-TTPF)”

Internet Security Alliance, “The ISA Guidelines for Securing the Electronics Supply Chain (Draft Version 6)”

NIAP, “Common criteria - Community NIAP Vision 11-10

NIAP, “Customers Perceptions about the Relevancy of Common Criteria for Supply Chain Security”

Intel/Cisco, “A CC Community for Supply Chain Common Criteria: Embrace, Reform, Extend’

Department Of Homeland Security, “Software Supply Chain Risk Management and Due-Diligence

Intel, “WarGames: Serious Play that tests Enterprise Security”


X-SCM pp. 79-103


IBM Global Business Services, “Supply Chain Risk Management: A Delicate Balancing Act”

Palisades Software Company, “Guide to Using @Risk, Risk Analysis and Simulation Add-In for Microsoft® Excel Version 5.7” (downloadable from Palisade.com website, click on Support > Product Manuals > @Risk Pdf Format).

Required Software:
For an introduction, please access the following resources:

A great way to be introduced to @RISK is to watch the “2 Minute Overview,” which is the first video in the @RISK tutorial series: http://www.palisade.com/risk/5/tips/en/gs/0.asp.

Download “Guide to Using @Risk, Risk Analysis and Simulation Add-In for Microsoft® Excel Version 5.7” (downloadable from Palisade.com website, click on Support > Product Manuals > @Risk Pdf Format).

@Risk Video Tutorial: Getting Started in @RISK (viewable from Palisade.com website, click on Support > Video Tutorials> @Risk.

IV: Content Of Modules

Module 1: The Cyber Supply Chain Security Landscape (Sessions 1 & 2)

Session 1: We will review the Global Risk Landscape for the ICT Industry and the extreme volatility that is characterizing the operating

We will cover the basic concepts and strategic importance of cyber supply chain risk management to corporate survival. We will closely examine the crucial role of cyber supply chain risk management capabilities through a case study of two electronics hardware producers—Nokia and Ericsson— and their differing responses to a devastating fire at their shared supplier, Philips; and a more detailed case about the long term lessons learned that Ericsson took away from the experience.

ICT Industry Case Questions:

1. What were key differences between Nokia and Ericsson in anticipating and responding to the critical supply chain risks they shared and how did these differences determine the outcome of the competitive struggle between them?

2. What were Ericsson’s lessons learned from the experience with the Philips Fire and how did it seek to better manage supply chain risks? How did Ericsson organize its SCRM program? What is the role of the Risk Council? How does Ericsson identify, classify and rate the impact of risks at suppliers? How does the company use contracts to manage risks?
Session 2: Our Guest Speaker will be Mr. Tyson Storch, director of Microsoft’s Trusted Supply Chain Initiatives  (To prepare for his talk, please read X-SCM pp.114-151)

Module 2: Enterprise Risk Management (Sessions 3-5)

Session 3: We will review the characteristics of Cyber Supply Chain Enterprise Risk Management; and cover emerging ERM Standards developed by NIST, the Institute Of Risk Management et al. We will introduce the Strategic Cyber-Supply Chain Risk Management Plan Exercise, a team-based project that reviews the strategic risk landscape and principal strategic, industry and company risks of a specific ICT organization and potential prevention, mitigation or recovery responses. We will distribute and discuss a detailed template for this report in class. Each team will be required to produce a report and presentation in the final session of the class.

Session 4: Guest speaker will be Mr. Jon Boyens, Program Director, SCRM, IT Laboratory, National Institute Of Standards and Technology. (To prepare for his talk, please read X-SCM pp.169-226: Cyber-Supply Chain Reference Model.)

Session 5: We will learn through a comprehensive case study how a best practice ICT organization (Cisco) has become more resilient through aggressive adoption of a formal corporate supply chain risk management programs.

Case Questions:

1. What were the principal strategic, industry and company level risks that Cisco faced? How did Cisco build a corporate program to systematically identify, prioritize and manage the principal risks they faced?

2. What obstacles did they face and how did they overcome them?

Module 3: SCRM Tools/Techniques (Sessions 6-9)

Session 6: We will also explore how leading industry organizations- Safecode for the software industry, ISA for internet services and the Supply Chain Council for the hardware industry- are systematically building risk assessment tools to help guide cyber supply chain risk management analyses. We will read the final report of the SCOR SCRM task force; and will also read X-SCM pp 79-103, which is written by the two co-leads of the SCOR SCRM task force.

Sessions 7 and 8: We will examine a range of tools for identifying, assessing and prioritizing ICT risk, with an emphasis on gaining exposure to the use of @Risk Software for Monte Carlo Risk Simulation Development.

Session 9: Strategic Cyber Supply Chain Risk Management Plan: each team will present its plan for a candidate company or organization

V. Grading
Final Exam--40 points

Strategic Cyber Supply Chain Risk Management Plan Exercise-50 points

This is a team exercise to conduct a comprehensive risk assessment and mitigation plan for a corporate ICT supply chain. Each team will select the candidate corporate supply chain that it will analyze; prepare a report; and present in class.

Student Participation-10 points

Participation points will be awarded for class attendance, engagement in class discussions and in teamwork.

PUAF 689F – Information Technology Acquisition in the Federal Government:

I. Purpose of Course:

Information technology (IT) offers inestimable capability, and has been leveraged extensively in federal government business systems, as well as virtually in all government operations. As a proportion of both functionality and cost, information technology now represents a significant part of all acquisition programs underway today. By all indication, this proportion will only increase in the future, as the government continues to transform its operations and business systems.

The government’s goal is to acquire these systems quickly and cost effectively. However, this goal is rarely achieved, since the deliberate process through which information technology and systems are acquired does not generally keep pace with the rapid pace of development in today’s information age. Therefore, improving acquisition of IT systems is critical to provide the required capabilities in an effective and efficient manner.

This course provides an overview of federal IT acquisition. Specific focus will be on the scope of acquisition, including organizational structures, regulations, and issues of acquisition processes and management, from the development of an initial capability or need, through design, development, production, fielding, sustainment, and disposal. The course also introduces the principles and concepts that underlie the successful acquisition of secure IT systems that offset risk by the acquiring entity. These include a review of vulnerabilities, threats, and security standards.

II. Key Course Learning Objectives:

Successful students will be able to:

1. Describe the federal acquisition environment, to include the applicable laws and regulations, and processes.
2. Understand the key challenges typically encountered during the contracting for, and while managing, federal IT projects.
3. Learn the differences and applicability of various software development models.
4. Articulate the primary threats to government cyber systems.
5. Differentiate between compliance that COTS vendors undertake for compliance versus risk management undertaken by the acquiring agency.
6. Describe the top five acquisition product related acquisition obstacles in detail.

III. Course Assessment:

- **Issue Papers (each of 3)** 45%
  The three short (four pages max) “issue papers” based on a selected IT acquisition issue. They should be clearly written, well thought out, and with appropriate facts (well researched and referenced) to support the student’s recommendations and conclusion.

- **Final Exam** 30%
  The final exam will be comprised of four essay questions that relate to the learning objectives.

- **Individual class participation (including an oral presentation of one of the papers)** 25%

*BULM 758P - Capstone – Cybersecurity Leadership:*

**I. Purpose of Course:**

Cyber security assurance has become a key ingredient to organizations in always connected world. This Capstone course on Cyber Security builds on the background from other foundational courses in the Cyber Security Leadership Certificate program and utilizes team-based consulting projects to provide students with methodologies and hands-on experiments for diagnosing and solving real-world cyber security and information assurance problems. Students are organized as consulting teams to companies that need to analyze a variety of cyber security scenarios and problems. This includes but not limited to: (1) Digital information assurance and forensics, (2) Assurance in hardware and software cyber supply chain, (3) Assurance in networked systems, and (4) Integrated systems. They are expected to analyze the situations, develop solutions, and present to cyber security clients.

Solutions may be defensive or offensive addressing how to disrupt, defend, or provide assurance to systems utilizing technology, process, policy, legal, or economic means. Considering the diversity of real-world problems on cyber security, we envision that the course will consist of three time periods of about equal length, and students will rotate between 2-3 consulting projects to gain experiences with balanced breadth and depth.

**II. Key Course Learning Objectives:**

- Employ general methodologies and integrate the learning in the Cyber Security Leadership program to analyze cyber security problems in practice;
- Reference known theories, models, or technologies in their proposed solutions to practical problems. Correctly recognize clients' needs and practical constraints, properly prioritize objectives, and recognize dependencies and tradeoffs among multiple objectives/criteria;
- Develop solutions to a variety of cyber security scenarios within practical constraints,
• Evaluate the strength, limitations, and tradeoffs of alternative solutions, and conduct risk assessments during projects to appreciate current systems’ liabilities or robustness of solutions proposed;
• Communicate the cyber security solutions effectively to a diverse audience, including those not familiar with technical details.

III. Readings:

A. Textbook and Reading Material

Government publications (NIST, DoD)

IV. Course Organization

Considering the diversity of real-world problems on cyber supply chain assurance, we envision that the course will consist of three time periods of about equal length, and students will rotate between 2-3 consulting projects to gain experiences with balanced breadth and depth. This rotation model mimics the medical school training, and similar practice has also been carried out successfully in engineering and science education.

Each rotation project may last 3-4 weeks, and be carried out in teams. The majority of students will rotate among three consulting projects.

    Session 1: Introduction and Course Organization
    Session 2-4: Rotation Project 1
    Session 5-7: Rotation Project 2
    Session 7-10: Rotation Project 3

* For students who have keen interests to explore in greater depth along a particular line of cyber supply chain assurance, after the first two rotations, they may choose to extend investigations on one of the two project areas that they have worked on. Students choosing this option must provide a 2-3 page proposal to outline the rationale and plan, and gain instructor’s approval by the mid-point of their second rotation project. We may defer this after 1st offering to simplify logistics and gauge students’ interests in this option.

V. Pool of Rotation Projects

The pool of the Capstone rotation projects will be expanded in stages. We envision that there will be 3-4 projects to start with in the first two years of offering. Some of the projects will utilize a multi-nodal Virtual Cyber Lab in partnership with key corporate and governmental partners such as SAIC.

Project 1: Digital Information Chain (Data Provenance)
“Digital Media Forensics: Empowering Sherlock Holmes in the Digital Era”

Candidate Instructor/Advisor: Min Wu (UMD)

Technology advancement and widespread use of digital multimedia devices in cyber supply chain management have brought about a number of forensic and provenance questions, including by what device an image was generated; where an image was from; what has been done on the image since its creation, by whom, when and how. Invisible traces are being explored by the technical community to manage and protect multimedia information and devices in the digital era.

A major type of traces, or digital fingerprints, addresses unauthorized leak and re-distribution of multimedia data. A unique signal or ID representing a receiving user is first embedded into the media data and then the fingerprinted content is distributed to the user. These track-and-trace fingerprints should be resilient to not only attacks mounted by an individual, but also attacks by multiple users, who work together to generate a new version to remove their fingerprints and circumvent the protection. Collusion-resistant fingerprinting finds applications ranging from military and government operations to piracy deterrence for copyrighted multimedia.

Complementing the above approaches that rely on proactive data embedding, an emerging type of fingerprints explores inherent traces left by the devices or processing systems a multimedia document has gone through. By employing such "intrinsic fingerprints", we can perform non-intrusive forensic analysis to determine the origin and processing history of digital images and other media source.

Student teams will be presented with problem scenarios on digital media forensics and carry out hands-on analysis on these digital fingerprints. The project may involve a combination of hands-on demo/lab tasks and programming tasks. The former may be constructed by adapting some research prototypes without explicit programming from students, allowing students to utilize technologies as a blackbox to observe and report their findings. The weight of each type of tasks depends on the student cohort’s technical background and capabilities.

Programming platform: Matlab, and/or C/C++/Java.

Equipment required: PC, digital camera and scanner.

A basic technical background and capability is expected/assumed from the students??

Project 2: Hardware Chain

Map supply chain network
Identify critical nodes
Perform risk & threat analysis
Determine countermeasures

Project 3: Software System Chain
Trace provenance and pedigree of software

Analyze confluence of legal underlying legal framework (contracts, licenses)

Develop CWRAF model for software application/market

**Project 4: Integrated System**

Map supply chain network (hardware, software, digital information)

Perform risk & threat analysis

Develop governance model

Develop incident response model

**VI. Course Grading:**

Three Units of Capstone Mini-projects 30 each

For each unit:

- Quality of Technical Deliverables (solutions, simulation etc) 15
- Project Report with Critical Discussions 10
- Class/Team Participation 5

**Final Presentation and peer reviews** 10
Appendix B

DRAFT
Midterm Exam – Systems & Design Thinking for Cybersecurity

Instructions
This exam is worth 100 points. First, please write out an sign the honor code first. Then, please answer each of the four questions that follow the honor code. Be sure to show you work so that you may receive partial credit.

Honor Code
Please write out and sign your name to the University of Maryland Honor Code

Question 1 (25 points)
Imagine you are Chief Information Security Officer of a financial services company. One of your technicians decides to upgrade a module found on your enterprise server to close a potential security flaw. This employee’s position description and role within the organizational hierarchy gives him the authority to make this decision autonomously. Unfortunately, this upgrade has some unintended consequences. Namely, a new security hole is now opened that did not previously exist. Fortunately, a technician in another part of the company just happened to learn of this upgrade over lunch and brought it to your attention. Does this current upgrade process embody the systems approach? Why or Why not? If yes, describe how it can be improved. If not, describe a better approach that would be more consistent with a systemic approach.

Question 2 (25 points)
Building on the hypothetical example in question 1, imagine that your CEO asks you to build a model of the company’s information system in order to identify potential security weaknesses. Using a systems modeling approach, should your model include the following components?:

- information flows
- business processes
- human processes
- capital flows
- physical flows
- physical processes

For each component, please describe why or why not it should be included in the model.

Question 3 (25 points)
Draw a diagram that shows an information process of a linear system (such as sending an email or fetching a web page) with no feedback. Show an improved process that includes at least one feedback loop. Describe the advantages (or disadvantages) of this feedback loop in your system.
Question 4 (25 points)
Recall one of the team presentations in class (this may be either your team’s presentation or another team’s presentation). Describe how the presentation may be further improved by using a systemic approach. Be sure to cite specific examples within the presentation. It is possible that this systemic approach is less desirable? If so, why? If not, why not?
THINK
Our consistently top-ranked faculty bring game-changing research into the classroom and the boardroom for maximum impact.

ANSWER
We challenge students to test their skills and knowledge in real-life situations, be entrepreneurial, create social value, and solve problems facing today's global organizations.

GROW
Our curriculum creates competitive, compassionate leaders and managers to compete globally across disparate cultures and disappearing borders.

CONNECT
Our students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

VISION
The Robert H. Smith School of Business will provide thought leadership to students, corporate executives and policymakers to equip them for impact in the world as agents of both economic prosperity and transformative social change.

OUR CORE VALUES
CREATIVITY, INNOVATION AND ENTREPRENEURIAL SPIRIT
Innovation with a purpose brings value, and creating value is at the heart of the enterprise. At Smith, we value innovation and entrepreneurship as keys to business education in the modern world.

INTEGRITY AND ACCOUNTABILITY
Integrity and accountability are essential to free markets and the conduct of global business, and are cornerstones of the Smith community.

A GLOBAL VIEW EMBRACING DIVERSITY
The world is increasingly more interconnected. This requires an understanding of and an appreciation for cultures and people beyond the school’s walls. At Smith, we value the rich contribution of people of many backgrounds and perspectives, and recognize that excellence cannot be achieved without diversity.

OUR STRATEGIC GOALS
To achieve our vision, the Smith School will:

- Grow future leaders to address global issues
- Generate thought leadership through high-impact research
- Connect with external communities
- Maintain world-class business school operations

GOALS

Our consistently top-ranked faculty bring game-changing research into the classroom and the boardroom for maximum impact.

How students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

THINK

We challenge students to test their skills and knowledge in real-life situations, be entrepreneurial, create social value, and solve problems facing today's global organizations.

ANSWER

Our curriculum creates competitive, compassionate leaders and managers to compete globally across disparate cultures and disappearing borders.

GROW

Our students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

CONNECT

The Robert H. Smith School of Business will provide thought leadership to students, corporate executives and policymakers to equip them for impact in the world as agents of both economic prosperity and transformative social change.

VISION

Our consistently top-ranked faculty bring game-changing research into the classroom and the boardroom for maximum impact.

How students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

THINK

We challenge students to test their skills and knowledge in real-life situations, be entrepreneurial, create social value, and solve problems facing today's global organizations.

ANSWER

Our curriculum creates competitive, compassionate leaders and managers to compete globally across disparate cultures and disappearing borders.

GROW

Our students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

CONNECT

The Robert H. Smith School of Business will provide thought leadership to students, corporate executives and policymakers to equip them for impact in the world as agents of both economic prosperity and transformative social change.

VISION

Our consistently top-ranked faculty bring game-changing research into the classroom and the boardroom for maximum impact.

How students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

THINK

We challenge students to test their skills and knowledge in real-life situations, be entrepreneurial, create social value, and solve problems facing today's global organizations.

ANSWER

Our curriculum creates competitive, compassionate leaders and managers to compete globally across disparate cultures and disappearing borders.

GROW

Our students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

CONNECT

The Robert H. Smith School of Business will provide thought leadership to students, corporate executives and policymakers to equip them for impact in the world as agents of both economic prosperity and transformative social change.

VISION

Our consistently top-ranked faculty bring game-changing research into the classroom and the boardroom for maximum impact.

How students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

THINK

We challenge students to test their skills and knowledge in real-life situations, be entrepreneurial, create social value, and solve problems facing today's global organizations.

ANSWER

Our curriculum creates competitive, compassionate leaders and managers to compete globally across disparate cultures and disappearing borders.

GROW

Our students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

CONNECT

The Robert H. Smith School of Business will provide thought leadership to students, corporate executives and policymakers to equip them for impact in the world as agents of both economic prosperity and transformative social change.

VISION

Our consistently top-ranked faculty bring game-changing research into the classroom and the boardroom for maximum impact.

How students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

THINK

We challenge students to test their skills and knowledge in real-life situations, be entrepreneurial, create social value, and solve problems facing today's global organizations.

ANSWER

Our curriculum creates competitive, compassionate leaders and managers to compete globally across disparate cultures and disappearing borders.

GROW

Our students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

CONNECT

The Robert H. Smith School of Business will provide thought leadership to students, corporate executives and policymakers to equip them for impact in the world as agents of both economic prosperity and transformative social change.

VISION

Our consistently top-ranked faculty bring game-changing research into the classroom and the boardroom for maximum impact.

How students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.

THINK

We challenge students to test their skills and knowledge in real-life situations, be entrepreneurial, create social value, and solve problems facing today's global organizations.

ANSWER

Our curriculum creates competitive, compassionate leaders and managers to compete globally across disparate cultures and disappearing borders.

GROW

Our students benefit from the school’s prominence in the Washington, D.C.-Baltimore, metropolitan region and our strong connections with federal, state and local government, national and international non-governmental agencies, and the social sectors, Northern Virginia and Baltimore’s high-tech and biotech corridors, and Baltimore’s banking, manufacturing, legal and health-care industries.
GROW FUTURE LEADERS TO ADDRESS GLOBAL ISSUES

For students to have a real impact after graduation, they need hands-on experience solving real-world problems; meaningful global opportunities; and the ability to be innovative and entrepreneurial in an environment that is marked by diversity—of races, cultures, incomes, genders and expectations. They must be able to use both qualitative and quantitative thinking in their approach to solving ambiguous, complex challenges. The Smith School will offer a systemic and systematic business education with a rigorous approach to teaching a wide range of fields. The Smith School will create influential new knowledge to contribute to the important issues of today and tomorrow—issues such as the global financial crisis, global climate change, emerging innovations in health, bio-tech and green technologies, cybersecurity and data integrity, the future of global marketing and digital business, ethical leadership and new governance structures, and disruptive and humanitarian supply chains. Our centers of excellence and executive education programs will help to transfer our thought leadership to practitioners and policymakers. We will vigorously recruit, retain and support faculty of the highest quality.

CONNECT WITH EXTERNAL COMMUNITIES

The Smith School will significantly expand its interactions with business and policy leaders, private-sector companies, governments both at home and abroad, the nonprofit sector, and especially with our alumni and friends. Working as partners with the Smith community, we will build greater pride in the Smith School and more widely and effectively communicate our successes. The quality and frequency of our outreach activities—including executive education, corporate relations, development and alumni relations, placement services, and marketing communications—will positively influence the school's brand and reputation.

GENERATE THOUGHT LEADERSHIP THROUGH HIGH-IMPACT RESEARCH

The Smith School will create influential new knowledge to contribute to the important issues of today and tomorrow—issues such as the global financial crisis, global climate change, emerging innovations in health, bio-tech and green technologies, cybersecurity and data integrity, the future of global marketing and digital business, ethical leadership and new governance structures, and disruptive and humanitarian supply chains. Our centers of excellence and executive education programs will help to transfer our thought leadership to practitioners and policymakers. We will vigorously recruit, retain and support faculty of the highest quality.

BENCHMARKS

Fall 2011: Launch new undergraduate curriculum, with more course content on ethics, corporate social responsibilities, globalization and problem-solving skills.

Fall 2011: Increase quality and type of MS programs with the launch of new certificate, several new joint programs, new research with experiential learning through challenging projects, and developing competency in social marketing and entrepreneurship.

By fall 2012, at least 50 undergraduate students and 90 MS students each year will have a global experience, including global study, trips and internships abroad.

By fall 2013, double the size of the full-time MBA program to 400-420 students.

Increase the diversity of the student body by increasing the percentage of African American, Hispanic and American Indian undergraduate and MS students.

BENCHMARKS

Fall 2011: Rank among the top 10 business schools in research by both the Financial Times and Bloomberg Businessweek.

Faculty will emerge in leadership positions in their academic fields and gain awards and citations.

Faculty line every department's self-participation in ThoughtLeadership@Smith and appear in popular media outlets.

Each center will host at least one keynote address by a well-known or influential industry leader.

Increased engagement with young alumni and alumni participation overall in events and giving.

Thirty-five students graduate, place more than 45 percent of our full-time MBA students, with the percentage increasing to 50 percent by summer 2011.

Our Corporate Partners Program will have a portfolio of 25 partners by August 2012, and 35 partners by August 2013.

WHAT COMES NEXT: VALUES, BEHAVIORS, RELATIONSHIPS

Implementing our strategic goals will require a culture of collaboration, new resources, administrative efficiency, and relentless and sustained effort across our community. Faculty, staff and students must fully support our vision and educational mission. We must challenge each other to live by our core values, pursue our strategic goals, and become more deeply invested in the Smith brand. Our alumni are talented, influential, highly placed and eager to help us enhance our reputation. Their partnership will be crucial to achieving our vision.

MAY 2010-2011
Appendix D

R.H. Smith School Cyber Security Leadership Certificate Program:

Questionnaire For Assessing Applicant Qualifications

I. Technical Proficiency/Experience

1. Please describe which areas of cyber security expertise or technology you are particularly proficient in?

_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

2. Which professional certifications do you have in cyber security? (Check the ones that apply)

___________CISSP- certified information systems security professional

___________CSSLP- certified secure software lifecycle professional

___________GIAC-Global Information Assurance Certification

___________ISACA- certification for CISM- certified information security manager

___________ISA- information systems security auditor

___________Other (Explain): ________________________________________________

___________None (Comments): ______________________________________________

3. How and for how long have you applied your expertise/certifications in your work?

_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

41
II. Managerial Proficiency/Experience

1. Which areas of management or systems design/development are you particularly proficient in?
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

2. Which professional certifications do you have in management/acquisition
   _______ FAC-C-Federal Acquisition Certification In Contracting Program
   _______ DAWIA- Defense Acquisition Workforce Improvement Act Certification
   _______ CAPM- Certified Associate In Project Management
   _______ PMP-Project Management Professional
   _______ PMI –ACP-Agile Certified Practitioner
   _______ PMI-RMP- Risk Management Professional
   _______ PMI-SP- PMI Scheduling Professional
   _______ Other (Explain):________________________________________________________________________
   _______ None (Comments):_______________________________________________________________________

3. How and for how long have you applied your expertise/certifications in your work?
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

IV. Leadership Potential

1. In your experience, what separates a manager and a leader in cyber security?
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
2. What are the essential leadership skills in the cyber-domain? Why you believe these are the right skills?

_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

3. How have you demonstrated those leadership skills in the workplace? Provide one concrete example where you showed leadership in the face of adversity and resistance and tell us your key lessons learned from it?

_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

V. Career Goals

Describe how you see your career progressing in the cyber security field and how this certificate will position you for future career opportunities?

_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________

Where do you see yourself making unique contributions to the field of cyber security?

_____________________________________________________________________________________
_____________________________________________________________________________________
_____________________________________________________________________________________
Appendix E

The Cybersecurity Market in the DC/MD/VA region

2011 Federal Government Jobs Outlook
By Dona DeZube, Monster Finance Careers Expert

Cybersecurity Jobs Especially Secure

Hiring hot spots include the new Cyber Security Command at Fort Meade, Maryland, the suburban Washington, DC, home to the National Security Agency and the Defense Information Systems Agency. While the exact number of civil service, civilian and military workers the government is hiring for cybersecurity positions is classified, it’s in the thousands, says Ronald Sanders, senior executive advisor at Booz Allen Hamilton, a consulting firm based in McLean, Virginia.

“Any career with the word ‘cyber’ in it will have a long, lucrative future,” he predicts. “Every federal agency, without regard to mission, has a need for cybersecurity professionals because every agency has systems they have to secure and protect. It’s going to be a growth area because it’s of critical national importance in the civil service and the many contractors that support the federal government.”

Cybersecurity isn’t just for computer geeks either. “Critical thinking and analysis skills are sometimes more important than technical skills in these jobs, where connecting the dots is important,” Sanders says.


08.11

Career Focus: Cyber Security — A Growing Threat, a Growing Career

By John R. Platt

"America's economic prosperity in the 21st century will depend on cyber security," said President Barack Obama in May 2009.

In the two years since those words were spoken, the problem of cyber security has only gotten worse. Wherever you look, cyber crime is on the rise, threatening individuals' privacy, corporate coffers, government secrets, the security of financial institutions, the operation of national infrastructures, and much, much more.

But with the rise of these threats also comes opportunities, as new careers are opening up for people to protect us from hackers, cyber criminals, organized crime, and even terrorists. The field of cyber security
is growing in leaps and bounds, and by all accounts there are simply not enough skilled professionals to meet even the current need, let alone the need projected over the next five years.

As it stands, every industry is at risk and in need of cyber security experts to help mitigate that risk. "Cyber threats are everywhere," says Ronald Woerner, assistant professor at the College of Information Technology at Bellevue University. "Hackers target not only large companies, but also small and medium businesses, local government, and non-profit organizations. The latter are often left unsecured due to a lack of money and resources to properly secure their cyber environments."

Even as the number of threats rises, they are also evolving. Specifically, the rise of mobile devices and cloud computing opens up whole new areas for hacking to occur and creates new vulnerabilities for companies. "As more and more data is moving to the cloud, the number of 'unique information access points' is shrinking rapidly," says Rohit Nadhani, founder and CEO of Cloudmagic.com. "Imagine a situation when the company moves to the cloud for storing all their documents. Now if that central repository on the cloud is hacked, it is then much, much easier to get a plethora of information without a lot of additional effort."

The hacks themselves can cause numerous types of damage: they can cost companies money (sometimes a great deal of it), information, time, or even, ultimately, their reputation. And reputation, as we'll come back to later, is critically important in today's world.

**The Opportunities**

One of the biggest areas for potential cyber security professionals to find employment is in the government. "The U.S. government is currently on track to spend over $79 billion for financial year 2011 on information security," says Mike Meikle, CEO of the Hawkthorne Group. "They are the largest customer for information security professionals at the present time." Meikle says the next greatest levels of need are within financial institutions and the utilities/energy sector.

While government might have the most immediate need, some see tremendous growth for cyber security professionals elsewhere. "I think we're going to see a lot of job growth in the private sector," says Derek Manky, senior security strategist at Fortinet, who points out that one of Obama's initiatives is to work more closely with private industry.

Whether it is government or industry, "every sector is going to need expertise in the field," says Dr. Nada Marie Anid, dean of the School of Engineering and Computing Sciences at New York Institute of Technology. "Your regular IT department will need to have a division of people with cyber security expertise."
Consulting firms specializing in cyber security will play an important role in all of this. "Consultants are a major player in security," says Shane Bernstein, managing partner of Q, an IT staffing agency. "Big enterprise companies or government agencies will bring in professionals with niche skill sets."

There are also a variety of roles cyber security professionals can play in their field. "On our team, there are careers and positions open for all areas," says Manky. He says these include areas such as antivirus, reverse engineering, and mobile code analysis. "There are also specific opportunities for the vulnerability researchers, the ones finding the software security holes," he says.

Meanwhile, Anid points out that additional people will be needed on the legal side, as well as in the development of cyber security standards.

No matter where the jobs are, the need is expected to stay steady. "Our forecast is a significant growth in demand for skilled security people today," says Andrew Herlands, director of security strategy for Application Security, Inc., a database security company, who points out that there already there aren't enough pros to go around. "Tons of job openings have gone unfilled because there aren't enough people to fill them."

**Skills You Need**

Common in-demand skills for security professionals, according to Bernstein, include vulnerability assessment, source code review and analysis, penetration and intrusion testing, web app testing, secure system design and network discovery, as well as a background in policies and procedures.

Non-technical skills are also vital, says Woerner. "It's equally important that cyber security professionals also possess the non-technical soft skills such as written and oral communications, policy-writing, and leadership," he says. He also points out that since most security breaches are caused by human vulnerabilities, "understanding how people think and operate" is critical.

Working in cyber security sometimes means thinking like a detective. Indeed, some people working in the field started their careers in law enforcement. "I was a cop," says Steve Santorelli, who started with Scotland Yard's Computer Crime Unit and now works for the internet security research company, Team Cymru. "I taught myself the geek side of things. Now we're actually getting a few people going the other way, leaving industry and taking pay cuts to go back into law enforcement."

Dave Merkel, Chief Technology Officer of Mandiant, also started in law enforcement, which he says taught him the skills needed to do his job. "When you are responding to a breach, you're applying problem-solving skills, asking yourself 'did I figure it all out or am I missing something?' If you missed something, the bad guy is still there in your system."

Merkel says that Mandiant, which is having trouble finding enough candidates to fill its open positions, likes people who themselves like fast-paced, busy environments, as well as people who understand that
their job hours might be a bit unpredictable. "It's not a 9-to-5 job," he says. "The bad guys don't have a lot of respect for holidays and birthdays."

Getting Hired

Getting hired in cyber security often means making yourself known. "Attend cyber security meetings and conferences," says Merkel. "A lot of times, if you're really smart and you're good at what you do, ask someone you know in information security for a referral into their company. A known entity is always valuable to us."

That sense of trust is a common thread in the industry. "It's all about trust and people, more so than technology," says Santorelli. "The majority of the people I deal with on a daily basis are the same ones I was dealing with ten years ago."

Santorelli says it's a small community, so it can appear daunting for people trying to break in. He advises blogging, using Twitter, and contributing to public security efforts to get noticed. "Get your name and your face out there and make a contribution. There's nothing to stop someone from learning a debugging tool and posting your results out there; it's for the good of everybody."

Fortinet's Manky agrees with this approach. "Find the blogs that security experts are reading. Post comments. Join the mailing lists. Get your voice out there. Getting involved is one step closer to getting your foot in the door."

If you're already working in computer science, NYIT's Anid suggests looking for master's programs or shorter courses to get yourself acquainted with security issues. "There are going to be many training courses for anyone who wants to earn that skill or enhance their own education," she says.

The Career Does Have Some Risks

Despite the need, and the challenge the career provides, cyber security might not be for everybody.

For one thing, many cyber security careers will be with government agencies, a field some might find limiting. "For those who are familiar with private sector employment, working for a government client can be a bit of a shock due to the cultural and business environment," says Meikle. On the plus side, he says that government positions tend to be far more stable or "secure" than private employment.

Another challenge is that you might never get that satisfaction of actually stopping a bad guy for good. "Usually the number one priority is getting the bad guy out, managing the risk and exposure," says Merkel. It's less important to get the hacker caught and charged for his crime than it is to simply "make the pain stop." As such, he says, few cyber criminals are actually stopped for good. "If your strategy hinges on getting the bad guy, it's a bad strategy," he says. Instead, the job is more about solving a breach and preventing it from happening again.
Because the hackers never really go away, cyber security can sometimes be frustrating. "It's a never-ending battle," says Woerner.

**Conclusion**

Cyber security is "a fantastic career," says Team Cymru’s Santorelli. "From my perspective, it's a great place to be. You make a real difference. You really help people, but you don't need to wear body armor. But you still get the thrill of the chase with the investigation. You need to word things in the right way to inspire an investigation. You get to contribute to antivirus products. At the end of the day, you're part of the psychological deterrent."

Manky agrees. "It's a very hot industry. I never get bored."

**Additional Resources & Reading**

"Department of Homeland Security Seeks Cyber Pros" [NextGov]

"Cyber Security, the Next Frontier for NASA Engineers" [SC Magazine]


NYIT Cyber Security Conference (September 15, 2011)

Open Web Application Security Project (OWASP)

IEEE Security & Privacy Magazine

U.s. Military Expands state cyber Assets

Maryland’s federal assets will be significantly strengthened in the near future with the addition of important federal cyber security facilities and programs. Aberdeen Proving Ground will soon be home to the Army's Communication and Electronics Command (CECOM) and its substantial engineering and research capabilities that are locating to Aberdeen from New Jersey. And the U.S. Navy recently announced plans to establish the Fleet cyber command at Fort Meade.

Maryland’s military commands play an important role in defending our nation’s freedom. the state is home to 12 major military installations and four smaller “niche” facilities establishing national security; designing aircraft and energetic systems; testing ordnance weapons, combat vehicles, aircraft, avionics systems; performing biomedical research; providing medical care to the armed forces; and facilitating global telecommunications. With an increasing reliance on information, these defense installations have become primary users of cyber security programs.

_Maryland is the cyber security leader. We house many federal facilities most at risk of cyber attack._
have one of the nation’s most advanced technical workforces. And we are one of only a few states already at work in the field.

Anthony Brown Maryland Lt. Governor

There is definitely a sense of mission, duty and patriotism in the cyber community in Maryland.

Rick Lipscomb Boeing

Just with the federal presence, there is such an enormous amount of computing being done in Maryland. All of those resources are here—they’re not going anywhere.

steve Walker steve Walker & Associates/Informatics coalition

**Coming Soon To a Workplace Near You: Cyber Job Titles**

By Aliya Sternstein 12/13/11 05:30 pm ET

The Office of Personnel Management this spring will release a list of job titles comprising the federal cybersecurity career path, creating for the first time much-needed consensus on the skills required of the cyber workforce, Homeland Security Department officials told Nextgov on Tuesday.

The fundamental problem contributing to a human capital crisis in the embryonic field is the inability of agencies to agree on what constitutes a cyber professional, according to federal officials. Without a standard definition, current counts on staffing levels and skills gaps are misrepresentative, the Government Accountability Office reported last month. Until agencies are comparing apples to apples in terms of cyber jobs data, the Obama administration will flounder building a workforce large enough and capable enough to respond to growing threats from nation states, hacktivists and insiders, federal officials say.

Currently, several departments, including DHS and OPM, are collaborating to standardize roles and responsibilities for job seekers -- and IT managers. OPM is linking its existing "occupational series," a list of jobs in a particular line of work at all pay grades, to 31 cybersecurity specialty areas set by the National Institute of Standards and Technology, DHS officials said during a discussion sponsored by the Government Business Council, Nextgov's research arm.

"They will key to the specialty areas and that will bring consistency across the government," said Peggy Maxson, DHS director for national cybersecurity education strategy. Specialties include, for example, software engineering, information assurance compliance, legal advice and vulnerability assessment. Maxson told Nextgov the jobs data is expected to be available in the spring but she could not provide a specific release date.

**A Human Capital Crisis in Cybersecurity**

Technical Proficiency Matters

49
A White Paper of the CSIS Commission on Cybersecurity for the 44th Presidency

cochairs

Representative James R. Langevin Representative Michael T. McCaul Scott Charney  Lt. General Harry Raduege, USAF (ret.)

We do not start with a blank slate, as there are several initiatives attempting to address the issues of career paths and training of the cybersecurity workforce. Organizations and initiatives that can be leveraged going forward include the Department of Homeland Security, International Information Systems Security Certification Consortium, Information Systems Audit and Control Association, the Institute of Electrical and Electronics Engineers, the Department of Justice, Federal Bureau of Investigation, National Security Agency, Department of Defense, Federal Chief Information Officers Council, Office of Personnel Management, State Department, US Cyber Command and US Cyber Challenge.

It is the consensus of the Commission that the current professional certification regime is not merely inadequate; it creates a dangerously false sense of security for the following reasons:

• Individuals and employers are spending scarce resources on credentials that do not demonstrably improve their ability to address security-related risks; and

• Credentials, as currently available, are focused on demonstrating expertise in documenting compliance with policy and statutes rather than expertise in actually reducing risk through identification, prevention and intervention.

IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework. The EBK is a framework to map Information technology (IT) security competencies. DHS has included fourteen areas ranging from incident management through digital forensics. The EBK was developed as complimentary framework to existing efforts of the National Institute of Standards and Technology (NIST) or the Committee on National Security Systems (CNSS) guidance on IT security training. DHS built upon established work resources and best practices from the public and private sectors. The EBK is intended to be a resource tool for the public and private sectors as well as higher education in development of curriculum and training. (http://www.us-cert.gov/ITSecurityEBK)

INTERNATIONAL INFORMATION SYSTEMS SECURITY CERTIFICATION CONSORTIUM (ISC)2 (http://www.isc2.org)

Certified Information Systems Security Professional (CISSP) is an information security credential accredited by ANSI ISO/IEC Standard 17024:2003 accreditation and leads the industry in acceptance. This certification is included in the Department of Defense (DoD) Information Assurance Workforce Improvement Program. The CISSP curriculum includes ten Common Body of Knowledge (CBK)
information security topics. According to the (ISC)2, “the CISSP CBK is a taxonomy – a collection of topics relevant to information security professionals around the world. The CISSP CBK establishes a common framework of information security terms and principles that allow information security professionals worldwide to discuss, debate and resolve matters pertaining to the profession with a common understanding.” (Tipton; Henry. Official (ISC)2 Guidetothe CISSP CBK. Auerbach Publications. ISBN 0-8493-8231-9.)

ISACA (http://www.isaca.org/).

ISACA, originally known as the, “Information Systems Audit and Control Association,” ISACA has established the CoBIT auditing and control standards, which are widely recognized and used. ISACA offers the following:

- Certified Information Systems Auditor (CISA);
- Certified Information Security Manager (CISM);
- Certified in Governance of Enterprise (CGIT); and
- Certified in Risk and Information Systems Control (CRISC).

The SANS INSTITUTE (http://www.sans.org)

SANS is a graduate degree-granting education and research institution that also provides advanced security training and certifications. Its 120,000 alumni are the computer network defenders, penetration testers, security-savvy system operators, forensics experts, secure programmers, and managers in more than 20,000 organizations ranging from the NSA and the Defense Industrial Base to the FBI to banks to hospitals to universities.

CREST (http://www.crest-approved.org)

The United Kingdom has developed a model for hands-on certification in the form of its Council of Registered Security Testers (CREST) test for security penetration testers and is building a network of independent certifiers. CREST was created in response to the need for regulated and professional security testers to serve the global information security marketplace. CREST is a not for profit organization with the goal to represent the information security testing industry and offer a demonstrable level of assurance as to the competency of organizations and individuals within approved companies.

The INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE)

(http://www.computer.org/portal/web/guest/home)

The IEEE is an international non-profit, professional organization, which provides learning opportunities
within the engineering, research, and technology fields. The goal of the IEEE education programs is to ensure the growth of skill and knowledge in the electricity-related technical professions and to foster individual commitment to continuing education among IEEE members, the engineering and scientific communities, and the general public. The IEEE offers certification and training for software professionals. Their organization recognizes there is a gap between education and work requirements and attempts to verify the students’ understanding the fundamentals of software development practices. (http://www.computer.org/portal/web/certification/home).

IEEE certifications include:

- Certified Software Development Associate (CSDA); and
- Certified Software Development Professional (CSDP).

THE DEPARTMENT OF JUSTICE; FEDERAL BUREAU OF INVESTIGATION (FBI)

The FBI Academy at Quantico provides a cyber education training program for domestic law enforcement and counterintelligence. They train over 2,192 new FBI agents in basic cyber training with 783 FBI cyber agents with advance training and over 1,100 cyber taskforce agents. Currently, the Office of Justice Programs (OJP), Bureau of Justice Assistance (BJA) provides federal assistance for training for law enforcement officials. The Counter Terrorism Training and Resources for Law Enforcement non-profit organization does provide training for cybersecurity and privacy. (http://www.counterterrorismtraining.gov)

NATIONAL SECURITY AGENCY (NSA)

The NSA and the DHS have jointly sponsored the National Centers of Academic Excellence in Information Assurance (IA) Education (CAE/IAE) and CAE-Research (CAE-R) programs. The goal of the programs is to reduce vulnerabilities in our national information infrastructure by promoting higher education and research in IA. It is also attempting address the growing need of professionals with IA expertise in various disciplines. The designation of an institution as a CAE/IAE or CAE-R is valid for five academic years and then, the school must reapply. Students who attend these designated schools are eligible for scholarships and grants through DoD and DHS. (http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml)

Additionally, the NSA has an initiative underway which is working to qualifying cyber-warriors. Aspects of this initiative include defining the cybersecurity workforce and moving forward with education and training.

DEPARTMENT OF DEFENSE (DoD): DoD 8570.01-M, “Information Assurance Workforce Improvement Program.”

positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2. The DoD IA Workforce includes, but is not limited to, all individuals performing any of the IA functions described in the Manual. Additional chapters focusing on personnel performing specialized IA functions including certification and accreditation (C&A) and vulnerability assessment will be published as changes to the Manual. Also establishes IA workforce oversight and management reporting requirements to support DoD Directive 8570.1. DoD 8570.01-M establishes the following goals:

Develop a DoD IA workforce with a common understanding of the concepts, principles, and applications of IA for each category, specialty, level, and function to enhance protection and availability of DoD information, information systems, and networks;

- Establish baseline technical and management IA skills among personnel performing IA functions across the DoD enterprise;

- Provide warfighters qualified IA personnel in each category, specialty and level;

- Implement a formal IA workforce skill development and sustainment process, comprised of resident courses, distributive training, blended training, supervised on the job training (OJT), exercises, and certification/recertification;

- Verify IA workforce knowledge and skills through standard certification testing; and

- Augment and expand on a continuous basis the knowledge and skills obtained through experience or formal education. FEDERAL CHIEF INFORMATION OFFICERS (CIO) COUNCIL and the OFFICE OF PERSONNEL MANAGEMENT (OPM) The E-Government Act of 2002 (Section209) (http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf) and Clinger-Cohen Act of 1996 (Division E) (http://www.gpo.gov/fdsys/pkg/PLAW-104publ106/pdf/PLAW-104publ106.pdf) includes the requirement for the assessment of the competencies and skills of the federal information technology (IT) workforce. The purpose of the requirement is to analyze the needs of the federal government relating to IT and information resources management. Currently, the CIO Council’s IT Workforce Committee, in conjunction with the OPM, is working on the new workforce survey instrument. Additionally, they have identified eleven information security roles (See Appendix A, Federal Information Security Workforce Development Matrix: Roles Identifications, Definitions and Prioritization dated April 21, 2009) and have assigned priorities to the roles. They are working on developing a matrix similar to their efforts for project management. To date, there are two draft documents available: Systems Operations and Maintenance Professional and Chief Information Security Officer (See Appendix A, Information Security Workforce Development Matrix (DRAFT): Systems Operations and Maintenance Professional and Information Security Workforce Development Matrix (DRAFT): Chief Information Security Officer). Other Efforts That Could Make a Big Difference: As previously stated, there are several initiatives underway that can be leveraged to address workforce issues. The following initiatives identified by the Commission should be studied, as they initially appear to be addressing short and mid-term cybersecurity workforce issues such as training.
STATE DEPARTMENT

As discussed above, the State Department team is clearly demonstrating that skills do matter. They have instituted a training program for all new team members covering multiple levels of competency with extensive, hands-on training in their environment.

US CYBER COMMAND

The US Cyber Command (USCYBERCOM) is a subordinate unified command under the United States Strategic Command created by the Secretary of Defense on June 23, 2009 (See Appendix A, “Memorandum for Secretaries of the Military Departments, SUBJECT: Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations). USCYBERCOM includes responsibility for several organizations including: the Joint Task Force for Global Network Operations (JFT-GNO); Joint Functional Component Command for Network Warfare (JFCC-NW); and the Defense Information Systems Agency (DISA), which will provide technical assistance for network and information assurance. They are to coordinate computer-network defense and direct US cyber-attack operations.

DoD 8570.01-M Change 2 (released Spring 2010)

This release reflects the DoD’s commitment to continuous improvement in the IA Workforce Improvement Program. Change 2 emphasizes the Department’s intent that the IA Workforce Improvement Program rely on skills-based training aligned with operational needs. DoD components will be encouraged to construct training and certification regimes that develop and assess the skills necessary to provide effective IA capabilities. This emphasis, coupled with improved compliance metrics, will move the Department away from reliance on stand alone, prescriptive certifications as the primary compliance metric for IA Workforce training and certification.

UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE (UMUC)

(http://www.umuc.edu)

The University of Maryland University College (UMUC) has three new degree programs starting in Fall 2010. They are a Bachelor and Master of Science in cybersecurity and Master in Science in Cybersecurity Policy. The UMUC is the largest U.S. public university with approximately 94,000 enrolled, which includes 50,000 active duty military, reserves, dependents, and veterans.

NATIONAL COLLEGIATE CYBERSECURITY COMPETITION

(http://www.nationalccdc.org)

The mission of the Collegiate Cyber Defense Competition (CCDC) system is to provide institutions with an information assurance or computer security curriculum in a controlled, competitive environment to assess their students’ depth of understanding and operational competency in managing the challenges
inherent in protecting a corporate network infrastructure and business information systems. Competition has grown from 5 schools in 2005 to 63 schools across 8 regions in 2009.

CCDC Events are designed to:

• Build a meaningful mechanism by which institutions of higher education may evaluate their programs.

• Provide an educational venue in which students are able to apply the theory and practical skills they have learned in their course work

• Foster a spirit of teamwork, ethical behavior, and effective communication both within and across teams

• Create interest and awareness among participating institutions and students. DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA) (http://www.darpa.gov) The Defense Advanced Research Projects Agency (DARPA) mission is to facilitate research and development including the development of new technology and techniques for use by the military. One example is the recently completed program titled, “The Cyber Trust Program” which was to create the technology and techniques to enable trustworthy information systems by:

1. Developing hardware, firmware, and microkernel architectures as necessary to provide foundational security for operating systems and applications.

2. Developing tools to find vulnerabilities in complex open source software.

3. Developing scalable formal methods to formally verify complex hardware/software.

Next Steps: Recommendations

With all these activities underway, it is the Commission’s intention to give impetus to and leverage the existing effort and initiatives to move forward in a comprehensive manner. The current Administration is addressing the education of cyber professional as part of the Comprehensive National Cybersecurity Initiative, an unclassified description of which was released on March 2, 2010. The topic is included as Initiative 8:

Expand cyber education. While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950’s, to meet this
challenge.

(http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative)

By building on many of the activities underway, the Commission is recommending the following for both the Executive Branch and Legislative Branch of the Federal Government:

1. The President’s cybersecurity coordinator should sponsor an effort to create an initial taxonomy of cyber roles and skills (See Appendix B, Taxonomy of Roles, v5 Draft) that can be the basis for recruiting and training and provide a more specific target for the education and training community to drive curriculum development and a regime of professional certifications grounded in practical reality;

2. The Office of Management and Budget (under the leadership of the Chief Information Officer and the Administrator of Federal Procurement Policy) in conjunction with the National Institute Standards and Technology should ensure the skills matrix along with future certification and eventually licensing requirements, if appropriate, be included as “standards” in their http://checklists.nist.gov and develop any additional procurement language, if necessary for: PART 39-ACQUISITION OF INFORMATION TECHNOLOGY

1. The authority citation for 48 CFR part 39 continues to read as follows: Authority: 40 U.S.C. 121(c); 10U.S.C. chapter 137; and 42 U.S.C. 2473(c).

2. Amend section 39.101 by revising paragraph (d) to read as follows: 39.101 Policy. (d) In acquiring information technology, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations available from the NIST’s website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated. (http://www.whitehouse.gov/omb/assets/omb/memoranda/fy2008/m08-22.pdf)

3. The Chief Information Officers Council should modify its biennial survey of the Federal information technology workforce to elicit more granular information on the cybersecurity skill profile of that workforce and to identify gaps;

4. The Office of Personnel Management should draft an action plan to address “career path issues” in the Federal workforce including developing a separate job series similar to the existing professional services such as legal/medical/chaplain/mental health and/or adjust the law enforcement classification (agents with the power to carry weapons and make arrests) to also include special hiring authority where there is evidence of shortages, consider mandatory continuous training, and/or establishing an extensive probationary period for skills to be demonstrated on-the-job;

5. The Department of Homeland Security in conjunction with the Federal CIO Council should create the Cyber Corp Alumni group which would include the top 10 percent of the students who complete the program. As part of this initiative, the program for the alumni group would include specific set of benefits such as training on how to be a Chief Information Security Officer; networking
with top cybersecurity professionals; and other related topics;

6. Develop model legislative language to address potential workforce gaps (See Appendix C, Definition for Legislative Branch); and

7. The Department of Labor’s Bureau of Labor Statistics (BLS) should lead an interagency committee to develop Standard Occupational Classification (SOC) for cybersecurity workforce (http://www.bls.gov/soc/socmanu.htm). This committee work would build upon the taxonomy recommended in Item 1.

**High Priority 1. Chief Information Security Officer**- The Chief Information Security Officer (CISO) is responsible for the information security strategy within an organization. The CISO establishes, implements, and monitors the development and subsequent enforcement of the organization’s information security program (i.e., policies, procedures, security architecture standards, security awareness and training program, IT contingency plans, IT security compliance issues). The CISO leads the evaluation and assessment of the security program to ensure that all aspects are in compliance with security requirements, while understanding security threats and vulnerabilities to operations and the organization’s environment. The CISO is responsible for information security risk management (e.g., determines risk impact, establishes risk mitigation plans and programs, works with business owners to devise processes for risk assessment) within the organization. The CISO manages the incidents response program (e.g., identifies, reports, and remediates incidents).

2. **Systems Operations & Maintenance Professional**- The Systems Operations and Maintenance Professional supports and implements the security of information and information systems during the operations, maintenance, and enhancements phases of the systems development life cycle. The Systems Operations and Maintenance Professional is also responsible for implementing server configurations, operating systems, database systems, firewalls, patch management, and account management to protect the systems against threats and vulnerabilities.

3. **Network Security Specialist**- The Network Security Specialist is responsible for examining malicious software, suspicious network activities, and non-authorized presence in the network to analyze the nature of the threat, and secure and monitor firewall configurations. The Network Security Specialist needs to understand the specimen’s attack capabilities, its propagation characteristics, and define signatures for detecting malware presence.

4. **Digital Forensics & Incident Response Analyst**- The Digital Forensics and Incident Response Analyst performs a variety of highly technical analyses and procedures dealing with the collection, processing, preservation, analysis, and presentation of computer-related evidence, and is responsible for disseminating and reporting cyber-related activities, conducting vulnerability analyses and risk management of computer systems and all applications during all phases of the systems development lifecycle. The Digital Forensics and Incident Response Analyst provides oversight of incident data flow and response, content, and remediation, and partners with other incident response centers in maintaining an understanding of threats, vulnerabilities, and exploits that could impact networks and
5. **Information Security Assessor**- The Information Security Assessor is responsible for overseeing, evaluating, and supporting compliance issues pertinent to the organization. Individuals in this role perform a variety of activities that encompass compliance from internal and external perspectives. These include leading and conducting internal investigations, helping employees to comply with internal policies and procedures, and serving as a resource for external compliance officers during independent assessments. The Information Security Assessor provides guidance and autonomous evaluation of the organization to management. This individual is responsible for planning and executing information systems operational assessment by obtaining, analyzing, and appraising competent evidential data for forming an objective opinion on the adequacy of information systems, procedures, and documentation. This individual also prepares, tests, and utilizes generalized computer audit software, programs, and questionnaires for accomplishing audit objectives and procedures.

**Medium Priority  6. Information Systems Security Officer**- The Information Systems Security Officer (ISSO) specializes in the information and security strategy within a system and is engaged throughout the systems development life cycle. The ISSO is charged with the development and subsequent enforcement of the company’s security policies and procedures, security awareness programs, business continuity and disaster recovery plans, and all industry and governmental compliance issues. The ISSO communicates with the business at the system level and understands security threats and vulnerabilities to the operations and the system’s environment.

7. **Security Architect**- The Security Architect is responsible for implementing business needs. The Security Architect supports the business function as well as technology and environmental conditions (e.g., law and regulation), and translates them into security designs that support the organization to efficiently carry out its activities while minimizing risks from security threats and vulnerabilities.

8. **Vulnerability Analyst**- The Vulnerability Analyst is responsible for detecting threats and vulnerabilities in target systems, networks, and applications by conducting systems, network, and web penetration testing. The Vulnerability Analyst identifies flaws that can be exploited to cause business risk, and provides crucial insights into the most pressing issues, suggesting how to prioritize security resources.

9. **Information Security Systems & Software Development Specialist***-The* Information Security Systems and Software Development Specialist is responsible for secure design, development, testing, integration, implementation, maintenance, and/or documentation of software applications (web based and non-web) following formal secure systems development lifecycle processes and using security engineering principles.

**FEDERAL INFORMATION SECURITY WORKFORCE DEVELOPMENT MATRIX: Roles Identification, Definition, and Prioritization**

**Low Priority  10. Chief Information Officer**- The Chief Information Officer (CIO) focuses on information security strategy within an organization and is responsible for the strategic use and management of
information, information systems, and IT. The CIO establishes and oversees IT security metrics programs, including evaluation of compliance with corporate policies and the effectiveness of policy implementation. The CIO also leads the evaluation of new and emerging IT security technologies.

11. Information Security Risk Analyst - The Risk Analyst is responsible for facilitating and developing data-gathering methods to control and minimize risks by understanding external threats and vulnerabilities to the operation and environment. The Risk Analyst analyzes vulnerabilities identified and implements best practices in their mitigation. This individual communicates compliance regulations and policies, monitors audit preparation practices, and implements risk management policies and procedures.

** The Information Security Systems & Software Development Specialist is an emerging role that was not rated on importance in the February focus group exercise. This role is classified under medium priority until further data and feedback can be obtained and analyzed.

Excerpted from research conducted by the Supply Chain Research Center, Robert H. Smith School of Business, University of Maryland, College Park and published by NIST, 2011
MEMORANDUM OF UNDERSTANDING (MOU)
Between
The Robert H. Smith School of Business, University of Maryland, College Park
and
The School of Public Policy, University of Maryland, College Park
March 30, 2012

This Memorandum of Understanding (MOU) is made by and between the Robert H. Smith School of Business (Smith) and the School of Public Policy (PubPol)

1. PURPOSE: Both parties wish to enter into this understanding to provide academic opportunities to students enrolled in the Certificate in Cybersecurity Leadership. It is understood that the purpose of the MOU between the Smith and PubPol schools includes: strengthening the quality and breadth of cyber security academic programs at both schools; leveraging the strengths and resources of programs at both schools; building and incentivizing the pool of qualified students equipped to enroll in the Masters’ of Engineering: Cybersecurity at Clark or the MS in Information Systems at Smith, by offering a rigorous program of Certificate study where nine (9) of the fifteen (15) earned credits can be applied to these advanced degrees.

2. BACKGROUND: Both institutions are deeply concerned with the need to address growing challenges in cybersecurity technology, and to equip technical experts with both cutting edge cyber knowledge and leadership skills that will allow them to contribute to enterprise-wide success. To better address these challenges, both schools are partnering to provide content for the Cybersecurity Leadership Program. Specifically, Smith wishes to leverage PubPol’s expertise in Federal IT Acquisition, making the Certificate attractive to the DC metro area federal and government contracting community.

3. This is a new MOU. Signing this MOU will join faculty, and stakeholders from the respective schools to cross-develop and cross-certify the Cybersecurity technology course of instruction within the Certificate in Cybersecurity Leadership program offered by Smith. Three (3) graduate-level course credits for the Federal IT Acquisition course and an additional six (6) credits for the Cybersecurity Technology course and the Certificate capstone (a total of nine (9) credits) may be transferred into the above listed Masters’s from Clark and Smith.

4. OBJECTIVE AND SCOPE:
The expectations from this MOU include the establishment of an authoritative definition of the body of knowledge in Cybersecurity Leadership; the collective development of state of the art teaching; a commitment to jointly market the program to federal and government contractor contacts; and equipping students to go on to attain a graduate level degree from Smith or Clark.
5. **SPECIFIC RESPONSIBILITIES/AUTHORITY**: The University of Maryland’s Robert H. Smith School and School of Public Policy designate the person(s) set forth in Section 6 as their respective representatives to coordinate and manage the activities under this MOU. The representatives shall meet as needed to discuss the programs, changes to programs, and any other topics of interest to either party.

Each party in this MOU retains full authority over and reserves the right to make changes in their respective courses, programs, and credential requirements. Each party shall publicize this MOU and programs mentioned herein in academic materials as appropriate and shall brief faculty and students as appropriate.

Each school agrees that all students must adhere to the rules and policies governing the degree awards in which they are engaged, including maintenance of satisfactory performance, and completion of the remaining credit hours inherent to the student’s specific degree program.

6. **COORDINATION CONTACTS**: The following persons will serve as points of contact at Smith and Clark and will communicate as needed by email and phone:

   Liz Barron  
   Senior Director, Custom Programs  
   Office of Executive Programs  
   Robert H. Smith School of Business  
   College Park  
   MD 20742

   lbarron@rhsmith.umd.edu  
   301 405 5387

   Anthony Savia  
   Assistant Dean, Finance and Administration  
   School of Public Policy  
   University of Maryland, College Park  
   MD 20742

   asavia@umd.edu  
   301 405 56335

7. **RESOURCES**:
   a. **Funding**: Smith will pay PubPol $661 in state and $1466 out of state per student enrolled in the Certificate in Cybersecurity Leadership in FY 13.
   b. **Manpower**: PubPol will pay the PubPol faculty member selected by PubPol to teach the 3-credit Federal IT Acquisition course at the PubPol faculty compensation rate. Smith will pay any other adjunct working on this course at the PubPol faculty compensation rate.
   c. **Marketing**: Comprehensive outreach is already in progress, involving efforts from Clark, SAIC and Smith. PubPol will partner in distributing eblasts (prepared by Smith) to PubPol contacts,
publicizing the program on its website, newsletters, and social media sites, and will provide faculty to support open houses or virtual info sessions as needed. PubPol will update Smith on its efforts and plan on a monthly basis throughout the term of the MOU.

8. EFFECTIVE DATE AND TERMINATION: This MOU will be effective from the date of signing and will have a duration of one year. Upon expiration of the one year, the MOU will be subject to renewal. Additions and changes to this MOU may be made at any time with the written agreement of both Smith and PubPol. Either party may withdraw from this understanding upon 60 days written notice to the other institution. Termination must be from the approving officials or their designated personnel.

9. APPROVAL: All parties identified below agree to the provisions and terms of this MOU.

APPROVED:

Liz Barron
Senior Director, Custom Programs
Office of Executive Programs
Robert H. Smith School of Business
College Park
MD 20742
lbarron@rhsmith.umd.edu
301 405 5387

Date: 3/30/12

Anthony Savia
Assistant Dean, Finance and Administration
School of Public Policy
University of Maryland, College Park
MD 20742
asavia@umd.edu
301 405 6335

Date: 4/12/2012

Donald F. Kett1
Dean
School of Public Policy
University of Maryland, College Park
MD 20742
Kett1@umd.edu
301 405 6083
April 15, 2012

Liz Baron  
Senior Director, Custom Programs  
Office of Executive Programs  
Robert H. Smith School of Business  
2419 Van Munching Hall  
University of Maryland  
College Park, MD 20742

Dear Liz,

With this letter, I want to underline our enthusiastic support for the proposed Certificate in Cybersecurity Leadership. We are very pleased to partner with the Smith School on this important initiative. Cybersecurity is unquestionably one of the major public policy issues facing the nation—and, indeed, the world—in this century, and this certificate is an important opportunity for the university to exercise strong leadership on the issue. The School of Public Policy’s considerable strength in cybersecurity will enhance the effort. This is precisely the kind of multi-disciplinary, cross-college effort that will mark the great successes of the university in the coming years.

Our joint agreement underlines our continuing commitment to presenting courses in the certificate and to sharing in ongoing conversations about the certificate’s growth and development. Our agreement recognizes, as well, the appropriate revenue-sharing arrangement that will ensure equity for the colleges involved in the certificate.

We are eager to launch this effort, and we’re very much looking forward to our partnership.

With best wishes,

Donald F. Kettl  
Dean
MEMORANDUM OF UNDERSTANDING (MOU)
Between
The Robert H. Smith School of Business, University of Maryland, College Park
And
The A. James Clark School of Engineering, University of Maryland, College Park

April 11, 2012

This Memorandum of Understanding (MOU) is made by and between the Robert H. Smith School of Business (Smith) and the A. James Clark School of Engineering (Clark)

1. PURPOSE: Both parties wish to enter into this understanding to provide academic opportunities to students enrolled in the Certificate in Cybersecurity Leadership. It is understood that the purpose of the MOU between the Smith and Clark schools includes: strengthening the quality and breadth of cybersecurity academic programs at both schools; leveraging the strengths and resources of programs at both schools; building and incentivizing the pool of qualified students equipped to enroll in the Master of Engineering - Cybersecurity at Clark or the MS in Information Systems at Smith, by offering a rigorous program of Certificate study where nine (9) of the fifteen (15) earned credits can be applied to these advanced degrees.

2. BACKGROUND: Both schools are deeply concerned with the need to address growing challenges in cybersecurity technology, and to equip technical experts with both cutting edge cyber knowledge and leadership skills that will allow them to contribute to enterprise-wide success. To better address these challenges, both schools are partnering to provide content for the Cybersecurity Leadership Program which it is hoped will feed students into the Master of Engineering - Cybersecurity at Clark, or the MS in Information Systems at Smith.

3. This is a new MOU. Signing this MOU will join faculty, and stakeholders from the respective schools to cross-develop and cross-certify the Cybersecurity Technology course of instruction within the Certificate in Cybersecurity Leadership program offered by Smith. Three (3) graduate-level course credits for this course, and an additional six (6) for the Federal IT Acquisition course and the Certificate Capstone (a total of nine (9) credits) may be transferred into the above listed Master of Engineering program from Clark.

4. OBJECTIVE AND SCOPE: The expectations from this MOU include the establishment of an authoritative definition of the body of knowledge in Cybersecurity Leadership; the collective development of state of the art teaching; and equipping students to go on to attain a graduate level degree from Smith or Clark.
5. **SPECIFIC RESPONSIBILITIES/AUTHORITY:** The University of Maryland’s Robert H. Smith School and A. James Clark School designate the person(s) set forth in Section 6 as their respective representatives to coordinate and manage the activities under this MOU. The representatives shall meet as needed to discuss the programs, changes to programs, and any other topics of interest to either party.

Each party in this MOU retains full authority over and reserves the right to make changes in their respective courses, programs, and credential requirements. Each party shall publicize this MOU and programs mentioned herein in academic materials as appropriate and shall brief faculty and students as appropriate. Each party will clearly state to students that successful completion of the certificate program does not guarantee admission to either Master’s program. Students must meet the admissions requirements of the program they intend to pursue.

Each school agrees that all students must adhere to the rules and policies governing the degree awards in which they are engaged, including maintenance of satisfactory performance, and completion of the remaining credit hours inherent to the student’s specific degree program.

6. **COORDINATION CONTACTS:** The following persons will serve as points of contact at Smith and Clark and will communicate as needed by email and phone:

   Liz Barron  
   Senior Director, Custom Programs  
   Office of Executive Programs  
   Robert H. Smith School of Business  
   University of Maryland, College Park  
   MD 20742  
   lbarron@rhsmith.umd.edu  
   301-405-5387

   Paul Easterling  
   Director, Educational Development and Communications  
   Office of Advanced Engineering Education  
   A James Clarke School of Engineering  
   University of Maryland, College Park  
   MD 20742  
   peaster@umd.edu  
   (301-405-3017)

7. **RESOURCES:**
   a. **Funding:** Smith will pay Clark the current campus tuition for Office of Advanced Engineering Education campus programs in each semester the course is offered (currently $752/credit) minus 10% off-campus tuition University overhead per student enrolled in the Certificate in Cybersecurity Leadership in FY 13.

   b. **Manpower:** Smith will pay the Clark faculty member selected by Clark to teach the 3-credit Cybersecurity Technology course at the Smith FY 13 faculty compensation rate.
8. **EFFECTIVE DATE AND TERMINATION:** This MOU will be effective from the date of signing and will have a duration of **one year**. Upon expiration of the one year, the MOU will be subject to renewal. Additions and changes to this MOU may be made at any time with the written agreement of both Smith and Clark. Either party may withdraw from this understanding upon 60 days written notice to the other school. Termination must be from the approving officials or their designated personnel.

9. **APPROVAL:** All parties identified below agree to the provisions and terms of this MOU.

**APPROVED:**

![Signature]

Date: 4/11/12

Greg Hanifee  
Assistant Dean  
Robert H. Smith School of Business  
University of Maryland, College Park  
MD 20742

(301) 405 7628  
ghanifee@rhsmith.umd.edu

![Signature]

Date: 4/11/12

Dr. George Syrmos  
Executive Director  
Office of Advanced Engineering Education  
University of Maryland, College Park

301-405-3633  
Email: syrms@umd.edu
Synopsis Cybersecurity Technology, Three credit course within Certificate in Cybersecurity Leadership, which may be applied to Master of Engineering - Cybersecurity

Cybersecurity Technology

September 29, 2012 - October 16, 2012

This course will discuss the main concepts of cybersecurity, demonstrating how leaders can build and guide resilience in their organizations. You will learn how to manage cybersecurity; the main security models; and how to evaluate cybersecurity. The course will also review how security is implemented in operating systems (Unix and Windows), databases, software, networks, web, and mobile devices.

Security approaches will be classified into prevention, detection and tolerance. Both the defense and the attacker perspectives will be addressed. Students will select a particular aspect of the cyber supply chain and investigate possible cybersecurity solutions. Students will present these solutions during class time and discuss them with other students. There will be a midterm and final exam.

Learning Objectives

- Recognize the significance of cybersecurity.
- Define approaches for securing various aspects of the cyber supply chain: the hardware, software and human level.
- Explore a particular aspect of the cyber supply chain and discuss how to secure it.
April 15, 2012

Liz Baron  
Senior Director, Custom Programs  
Office of Executive Programs  
Robert H. Smith School of Business  
2419 Van Munching Hall  
University of Maryland  
College Park, MD 20742

Dear Liz,

With this letter, I want to underline our enthusiastic support for the proposed Certificate in Cybersecurity Leadership. We are very pleased to partner with the Smith School on this important initiative. Cybersecurity is unquestionably one of the major public policy issues facing the nation—and, indeed, the world—in this century, and this certificate is an important opportunity for the university to exercise strong leadership on the issue. The School of Public Policy’s considerable strength in cybersecurity will enhance the effort. This is precisely the kind of multi-disciplinary, cross-college effort that will mark the great successes of the university in the coming years.

Our joint agreement underlines our continuing commitment to presenting courses in the certificate and to sharing in ongoing conversations about the certificate’s growth and development. Our agreement recognizes, as well, the appropriate revenue-sharing arrangement that will ensure equity for the colleges involved in the certificate.

We are eager to launch this effort, and we’re very much looking forward to our partnership.

With best wishes,

Donald F. Kettl  
Dean

Donald F. Kettl  
Dean

2101 Van Munching Hall  
College Park, Maryland 20742-1821  
301.405.6330 TEL  301.405.4675 FAX  
kettl@umd.edu
Appendix H

Professional Studies Cybersecurity Leadership Certificate Program Faculty

Sandor Boyson, PhD  
*Research Professor and Co-Director, Supply Chain Management Center & Academic Co-Director*  
Robert H. Smith School of Business, University of Maryland, College Park

Dr. Boyson currently serves as founding Co-Director, Supply Chain Management Center; and Research Professor at the Robert H. Smith School of Business at University Of Maryland College Park. He also served as the Chief Information Officer for the Business School for four years.

His new book on business risk management “X-SCM: The New Science Of X-Treme Supply Chain Management” (co-edited with Ms. Lisa Harrington and Dr. Thomas Corsi) is an official publication of the Council Of Supply Chain Management Professionals (Routledge/Taylor Francis, Fall, 2010).

His research project on Cyber-Supply Chain Risk Management (in collaboration with SAIC) has been featured at RSA 2010; and in Information Week (November, 2009). His policy research on “Unified Communications” was featured in the World Economic Forum’s 2008 Global IT Report. His ICT & Supply Chain research has also been disseminated in two previous books, “Logistics And The Extended Enterprise” (John Wiley, 1999) and “In Real Time: Managing The New Supply Chain” (Praeger, 2005); two World Bank monographs; a DARPA research paper on Net Centricity and numerous publications/citations in the Shanghai Daily; the Economist Intelligence Unit; CIO Magazine; Information Week; Fortune; the Harvard Business Review & the Journal of Commerce.

Hart Rossman  
*Vice President and Chief Technology Officer for Cyber Security Services & Solutions and Academic Co-Director*  
SAIC

Hart Rossman keeps SAIC’s cyber technologies ahead of new threats. He has oversight and responsibility for technology strategy, vendor relations and solution development, R&D, practice leadership for cyber security solutions; and provides customer support in solving all phases of complex information assurance-related problems.

Areas of technical expertise include risk management, security in the software and system development lifecycle, system certification and accreditation, and security in the cyber supply chain. Domains of focus include cloud, mobility, consumerization, big data and analytics, national security systems, and emerging technology & cultural trends.
SAIC’s cybersecurity experts are actively involved in research, innovation, and education. Rossman serves as a Senior Research Fellow within the Robert H. Smith School of Business at the University of Maryland in the area of Cyber Supply Chain Assurance and as a faculty member with the Institute for Applied Network Security.

Rossman’s work in the community includes representing SAIC’s Incident Response Team in FIRST, is a founding member of the Corporate Executive Programme, and he is on the steering committee of the Open Group’s Trusted Technology Forum; and is on UMBC’s Cybersecurity academic advisory committee.

He has co-authored seminal academic papers in the cyber supply discipline including “Building a Cyber Supply Chain Assurance Reference Model,” “Assessing SCRM Capabilities and Perspectives in the IT Vendor Community: Toward a Cyber Supply Chain Code of Practice,” and contributed to the book “X-SCM: The New Science of X-treme Supply Chain Risk Management.”

Rossman has been named to the state of Maryland Governor’s Workforce Investment Board Cyber Security Workforce Steering Committee as well as ISC2’s Application Security Advisory Board and is a named contributor to the CWE/SANS Top 25 Most Dangerous Software Errors.

Rossman has a BA and MBA from the University of Maryland College Park. He has earned CISSP and CSSLP certification.

Joseph P. Bailey, PhD
*Research Associate Professor, Decisions, Operations and Information Technologies*
Robert H. Smith School of Business, University of Maryland.

Dr. Bailey’s research and teaching interests span issues in telecommunications, economics, and public policy with an emphasis on the economics of the Internet. This area includes an identification of the existing public policies, technologies, and market opportunities that promote the benefits of interoperability. Bailey is currently studying issues related to the economics of electronic commerce and how the Internet changes competition and supply chain management.

He earned his PhD in Technology, Management and Policy, from the Massachusetts Institute of Technology and his MS from Stanford University, Department of Engineering-Economic Systems.

Michel Cukier, PhD
*Associate Professor of Reliability Engineering with a joint appointment in the Department of Mechanical Engineering and the Institute for Systems Research*
A. James Clark School of Engineering, University of Maryland, College Park
Dr. Cukier received a degree in physics engineering from the Free University of Brussels, Belgium, in 1991, and a doctorate in computer science from the National Polytechnic Institute of Toulouse, France, in 1996. From 1996 to 2001, he was a researcher at the University of Illinois, Urbana-Champaign. He joined the University of Maryland in 2001 as Assistant Professor.

His research covers dependability and security issues. His latest research focuses on the empirical quantification of computer security. He has published over 60 papers in journals and refereed conference proceedings in those areas.

William Lucyshyn

Research Director at the Defense Advanced Research Projects Agency (DARPA) and a Visiting Senior Research Scholar at the Center for Public Policy and Private Enterprise
School of Public Affairs at the University of Maryland, College Park

Bill Lucyshyn conducts research into the public policy challenges posed by the increasing role information technologies play in improving government operations and their relationships with the private sector. Previously, he served as a program manager and the principal technical advisor to the director, DARPA, on the identification, selection, research, development, and prototype production of advanced technology projects. Prior to this appointment, he completed a distinguished 25-year career in the U.S. Air Force serving various operations, staff, and acquisition positions.

Lucyshyn received his Bachelor Degree in Engineering Science from the City University of New York in 1971. In 1985 he earned his Master’s Degree in Nuclear Engineering from the Air Force Institute of Technology. He was certified Level III, as an Acquisition Professional in Program Management in 1994.

Dan Reddy

Senior Consulting Product Manager – EMC Product Security Office, RSA Security Division
EMC Corporation

Reddy leads the Supply Chain Assurance arm of the EMC Product Security Office where he has been a champion for promoting product integrity and outlining product requirements for Federal security compliance for the last five years. His 16-year career at EMC has included a variety of security, IT and educational roles. He was co-chair for SAFECode’s first whitepaper on Supply Chain Integrity Controls. He is co-chair of the Open Group’s Trusted Technology Forum’s Global Outreach and Acquisition workstream. He spent 15 years at New England Electric, a major utility with critical national infrastructure where he held a variety of IT and business roles. He teaches computer science at Quinsigamond Community College where he has taught for over three decades. He graduated from Tufts University with an education degree and holds two M. Ed. degrees from Worcester State College in education and computer science.
Min Wu, PhD  
_School of Electrical and Computer Engineering_  
A. James Clark School of Engineering, University of Maryland, College Park

Dr. Min Wu received a B.E. degree in electrical engineering and a B.A. degree in economics from Tsinghua University, Beijing, China, in 1996 (both with the highest honors), and an M.S. degree and Ph.D. degree in electrical engineering from Princeton University in 1998 and 2001, respectively. She was with NEC Research Institute and Signafy, Inc. Princeton, NJ, in 1998, and with the Media Security Group, Panasonic Information & Networking Laboratories, Princeton, NJ, in 1999. Since fall 2001, she has been a faculty member of the Electrical and Computer Engineering Department and the Institute of Advanced Computer Studies (UMIACS) at University of Maryland, College Park. She is also affiliated with the Institute of Systems Research (ISR) in the same university.

Wu's research interests include information security and forensics, and multimedia signal processing and communications. She has published one book "Multimedia Data Hiding" (Springer-Verlag, 2003) and about 65 refereed journal and conference publications. She holds four U.S. patents on media security. She is a member of the IEEE Technical Committee on Multimedia Signal Processing and on Multimedia Systems and Applications. She has served as publicity chair for 2003 IEEE International Conference on Multimedia and Expo (ICME’03), finance chair for 2007 IEEE International Conference on Acoustic, Speech, and Signal Processing (ICASSP'07), and in the technical program committees of several international conferences on multimedia, signal processing, communications, and information security. She also co-edited a Special Issue on Multimedia Security and Rights Management for EURASIP Journal of Applied Signal Processing in 2004.

She received an NSF Career award on information security and protection in 2002, and a George Corcoran Education Award from University of Maryland in 2003, a 2004 Best Paper Award from the EURASIP Journal of Applied Signal Processing, and a Young Investigator award on multimedia security and forensics from U.S. Office of Naval Research in 2005. In 2004, she was selected by the MIT Technology Review Magazine as one of the 100 top young innovators whose contribution to emerging technologies will profoundly influence the world.
Overview

The Robert H. Smith School of Business will utilize its technology capabilities to structure the Certificate in Cybersecurity Leadership in the form of three blended learning environments. Blended learning refers to the combination of different approaches and techniques used to deliver quality, yet convenient, learning environments where students and instructors engage in activities that promote virtual and face-to-face participation through collaboration.

Program Delivery Mechanisms

The approaches used to deliver the Certificate in Cybersecurity Leadership will include:

- Connecting students and instructors virtually by linking traditional face-to-face classrooms using multi-site high definition video conferencing from College Park to other satellite locations. This will be the primary launch delivery method for FY13.

- Connecting students from the location of their choice using laptops, iPads, or mobile devices to the instructor using a high definition videoconferencing room located in College Park. We will experiment with this method in launch year FY13 to inform future development of the program.

- Connecting students virtually via online web conferencing tools from the location of their choice using laptops, iPads, or mobile devices to traditional classrooms in College Park where the instructor and other students will participate face-to-face. This can be a useful alternative in launch year, and can also allow us to experiment as above.

Technical Requirements

- In the first scenario described above, the instructor will host the video teleconferencing (VTC) from a classroom in College Park and connect to other VTC units located at the satellite sites. There are no requirements for exact equipment at the endpoint side, however industry standard protocols such as H.323 are required. Audio and video components are distributed through the VTC or microphones in the classroom. We understand that Clark uses the VTC equipment at both the HEAT Center in Aberdeen, and the SMHEC in Patuxent and will continue to collaborate with Clark and their onsite contacts to ensure that the necessary quality of service is provided.

- In the second scenario, the instructor will host the VTC from a dedicated VTC room located in College Park. The students are provided a login, instructions and link to download an application to the device of their choice. Students will launch the application and connect to the virtual session. Audio and video are distributed through the VTC and local devices.

- In the third scenario, the instructor hosts an online web conference from a classroom in College Park. The students are provided with a login, instructions and a link to join the online web conference. Audio is distributed through the students' local devices, and classroom microphone system. Video of participants is displayed on the projection screen.
Resources and Fees

Technology continues to evolve around blended learning environments, distance education, and online learning communities. The stipulation for human resources to support the technology is a critical component for success. For budget purposes, we have assumed that we will use all three technology scenarios in launch year and that we may have to make a capital investment, if the need arises to extend past the current technology licenses and capabilities. These estimates are therefore “worst case scenario”.

All communications, servers and end-points will adhere to appropriate industry standard security controls.

Technology Resources

- There will be no cost for utilizing the school’s Cisco, Tandberg or Polycom multi-site VTC units located in College Park to connect up to 3 additional satellite sites. Additional costs would be incurred if the need arises to connect more than 4 sites.

  **Estimated one time capital investment cost of $18,000**

- The Robert H. Smith School has already acquired 25 licenses for Tandberg Movi application clients to support various consumer device connections to our dedicated teleconferencing suite. Additional costs would be incurred if the need arises to extend beyond 25 licenses.

  **Estimated one time minimum cost of $1,800 per user pack/or $72 per student**

- Adobe Connect and WebEx will provide web conferencing and collaboration features such as chat, whiteboard, recording, presentation and document sharing. Sessions can be recorded and stored on a secure server. Access to the virtual meetings and recordings will require authentication using standard campus security protocols such as use of CAS, campus directory, or local account credentials.

  **Estimated annual cost of $150 per course that can accommodate up to 100 participants**

- We will utilize the University’s Learning Management System to provide access to online course materials, syllabus, etc. Participants will authenticate using standard University security protocols.

Staff Support Resources

- College Park technical support per week for 18 weeks at $600 = $10,800

  **$400 per Saturday + $200 per Tuesday**

- Ronald Reagan technical support per week for 18 weeks at $360 = $6,480

  **$240 per Saturday + $120 per Tuesday**

- Patuxent Air Naval SMHEC remote location $1250 per student x 7 = $8,750

- Aberdeen Heat Center support $600 per student x 7 = $4200
Contingency Planning

The ability to mitigate the risk of service interruptions can be achieved through contingency planning. Technology systems are susceptible to a variety of disruptions, ranging from mild (e.g., short-term power outage, hardware failure) to severe (e.g., natural disasters). While it is virtually impossible to completely eliminate all risks, we have focused efforts on effective and efficient service recovery solutions.

- In the event of a VTC hardware failure, we have configured back-up VTC units that can be readily deployed by our technology support staff.

- In the event that a student or instructor encounters a hardware failure with their own device, we have established loaner pools of equipment at College Park and Ronald Reagan so they may reserve laptops, webcams, microphones, and headsets prior to class.

- In the event of a campus-building network outage, we have established a voice conferencing bridge whereby participants would dial a toll free 800# to join the class for discussion. Alternatively, we can invoke a web conference, as described above in the third scenario under Program Delivery Mechanisms, using a Verizon wireless access point.

- In the event of a power outage, or communications failure at any satellite site, we can invoke a recording of the session and make it available on a secure server for the students to view at their convenience.

In addition, contingency procedures will be reviewed and provided to program coordinators and technology support staff. They will include contact information for contingency planning team personnel; vendor contact information, standard operating procedures and checklists for system recovery or processes; equipment and system requirements lists of the hardware, software, and other resources required to perform recovery operations.