BOARD OF REGENTS

SUMMARY OF ITEM FOR ACTION
INFORMATION OR DISCUSSION

TOPIC: USM Cyber Security Task Force Recommendations

COMMITTEE: Economic Development and Technology Commercialization

DATE OF COMMITTEE MEETING: December 1, 2011

SUMMARY: Cyber Security is becoming increasingly critical for the U.S. economy, civic infrastructure, public safety and national security in today's globally interconnected communications and information environment. The Committee will be briefed on the May 2011 Report of the Cyber Security Task Force as well as the October 2011 Progress Report on the Recommendations.

ALTERNATIVE(S): This item is for discussion purposes.

FISCAL IMPACT: This item is for discussion purposes.

CHANCELLOR'S RECOMMENDATION This item is for discussion purposes.

COMMITTEE RECOMMENDATION: DATE:

BOARD ACTION: DATE:

SUBMITTED BY: Joseph F. Vivona (301) 445-2783

Report of the Cyber Security Task Force

to the University System of Maryland, May 2011

TABLE OF CONTENTS

Executive Summary

University System of Maryland (USM) Chancellor Dr. William E. Kirwan in November 2010 convened a task force of representatives from USM institutions, state and federal government agencies, and private-sector businesses to examine the assets of the USM in the area of cyber security and evaluate the workforce needs of government agencies and private industry in this area.

After meeting with representatives of USM institutions as well as federal agencies, the USM Cyber Security Task Force formed two subcommittees. One subgroup (Academic Inventory) inventoried all of the academic programs and university assets related to cyber security in addition to research and collaborative relationships with faculty, government and private industry. The second subgroup (Government and Industry) concentrated on assessing the types of skills and degrees most applicable in assisting government and private industry in meeting their workforce needs.

The Task Force found within the USM a range of programs—including 53 separate bachelor's degrees, 33 master's degrees, nine doctoral degrees and 13 related undergraduate and post-baccalaureate certificates—relating to a range of needs within the cyber sector.

Four USM institutions have been designated as Centers of Academic Excellence or Research Excellence in Information Assurance by the National Security Agency and the U.S. Department of Homeland Security: Towson University, the University of Maryland, Baltimore County (UMBC), the University of Maryland, College Park (UMCP) and University of Maryland University College (UMUC). USM institutions have significant and growing research programs in the area of cyber security, many including collaborations with the public and private sectors.

There is no doubt that the demand for a skilled workforce in the area of cyber security and information assurance is significant and will continue to grow. The Task Force was able to determine qualitative standards as to academic areas needed. However, without a more extensive scientific survey, a better quantitative statement on numbers of degrees is not possible at this time.

The Government and Industry subgroup developed a survey instrument to query for the basic skill set needed for the cyber workforce. The common thread between the feedback from all employers and discussions within the Task Force is that all graduates entering the job market, regardless of their major, need a basic awareness and understanding of cyber security. The USM would benefit employers as well as current and future cyber professionals by continuing to provide high-caliber degrees in traditional technology and policy areas, and the USM should enhance traditional curriculum with hands-on training and development in cyber techniques and technologies.

The Task Force made five actionable and achievable recommendations:

1. Working with the Governor's Workforce Investment Board, conduct a comprehensive and scientific survey of employer needs.

2. Enhance and extend higher educational offerings related to cyber security and information assurance.

3. Establish more partnerships among education and government and private industry and leverage the resources available.

4. Strengthen research and support innovation and technology transfer in cyber security.

5. Expand the cyber security career pipeline through collaborations between the USM and Maryland's community colleges. As part of this coordination, adopt models to increase awareness and reduce impediments to obtaining a security clearance.

The Task Force recognizes there are a number of ways to address cyber security and information assurance and believes the effort to do so should continue to expand by implementing the five recommendations proffered in this report.

University System of Maryland Cyber Security Task Force
Recommendations Progress Report
October 18, 2011

The Task Force made five actionable and achievable recommendations. Activities, programs and initiatives now taking place to respond to these recommendations are listed below.

1. Working with the Governor's Workforce Investment Board (GWIB), conduct a comprehensive and scientific survey of employer needs.

USM is working with Larry Letow (Tech Council of Maryland and GWIB member) and GWIB to use graduate student interns, GWIB and USM along with SAIC Corporation to do conduct this scientific survey this December.

2. Enhance and extend higher educational offerings related to cyber security and information assurance.

USM Institutions are continuing to add courses, tracks, certificates, training programs, and degree programs in computer science, information systems, information technology, information assurance, cyber security, cyber forensics, and engineering.

University of Maryland, College Park (UMCP) Professional Master's Program in Cybersecurity will be launched via the Office of Advanced Engineering Education in the Fall of 2012.
UMCP Business School Cyber Security Supply Chain Certificate Program starts Spring 2012.
UMCP Research Experience for Undergraduates in Cybersecurity-9 week NSF-sponsored cyber camp for undergraduate students, offered in Summer 2011.
Building on the existing university curriculum to add more academic courses in cybersecurity. Undergraduate students have the option to pursue concentrations in cybersecurity to complement their academic major. Students also have the opportunity to supplement their educational instruction by engaging in cybersecurity research through special programs with faculty, summer internships, and other research experiences for undergraduates.

The **University of Maryland Baltimore County (UMBC)** Center for Information Security and Assurance (CISA) promotes research, education, and sound internal practices in information security and assurance. It is administratively housed within the College of Engineering and Information Technology (CoEIT) and closely linked with the Department of Computer Science and Electrical Engineering (CSEE). This center facilitates interactions with other UMBC departments and entities, including:

- Information Systems (IS)
- Mathematics
- Physics
- The Public Policy Graduate Program
- Maryland Center for Telecommunications Research (MCTR)
- UMBC Continuing & Professional Studies

The Center has also facilitated interactions with local area businesses, laboratories, and government agencies. CISA was formally established in Fall 2001 within the Department of Computer Science and Electrical Engineering.

CISA hosts a free distinguished lecture series on information security and assurance open to the public. It also coordinates the Capital Area Seminar on Information Assurance. CISA's Cyber Defense Lab provides an isolated network of workstations available to UMBC students and faculty for research projects and classroom exercises.

Bowie State University (BSU): Bachelor's, Master's and Doctorate in Computer Science; MS in Management Information Systems with concentration in Information Assurance.
The Management Information Systems program was restructured in fall 2005 to realign the curriculum to the emerging needs of the market, according to Anthony Nelson, dean of the College of Business. The Information Assurance program is the latest change to enhance the curriculum and to train cyber security talent.

Frostburg State University (FSU): Track in Information Technology major; in 2006 added courses in ITEC 470 Security and Risk Management and ITEC 475 Computer and Cyber Forensics.

University of Baltimore (UB): Bachelor's in Applied Information Technology with courses in Information Assurance (COSC 432), Network Security (COSC 433)

UMBC: Training programs

Certificate Programs
Certificate in Cyber Foundations
Certificate in Cybersecurity
Certificate in Information & Network Security
Core Industry and DoD 8570 Certification Courses
- CompTIA: A+ Certified IT Technician | Network+ | Security+
- Certified Information Systems Security Professional (CISSP)
- System Security Certified Practitioner (SSCP)
- Certified Ethical Hacker (CEH)
- Cisco Certified Network Associate (CCNA)

Network Security and Administration
- Network and Packet Analysis
- Network Security Administrator (ENSA)
- Network Security (GL510)
- Enterprise Linux Security Administration (GL550)

Secure Software Development
- Certified Secure Programmer (ECSP)
- Java Development for Secure Systems
- Securing Java Web Applications
- Securing Java Web Services
- SOA for Security Professionals

Computer Forensics
- Computer Hacking Forensic Investigator (CHFI)

Penetration Testing
- Certified Security Analyst (ECSA)

Network Defense
- Persistent Attack and Exploitation: Offense
- Persistent Attack and Exploitation: Defense

Foundational and Specialty Skills
- Critical Thinking and Problem Solving
- Management for Technical Professionals
- ITIL v3 Foundation
- Capturing System Requirements
- Systems Testing and Quality Assurance
- Counterintelligence for IT Professionals

UMBC Degree Program
- UMBC Masters Degree of Professional Studies in Cybersecurity

Information Assurance Track in BS, MS, or PhD level: Computer Science (CMSC), Electrical Engineering (ENEE), Computer Engineering (CMPE), Information Systems (IS)

University of Maryland University College (UMUC) has established the following:
BS Cybersecurity
MS Cybersecurity
MS Cybersecurity Policy

- Graduate Certificates in: Foundations of Cybersecurity
- Cybersecurity Policy
- Cybersecurity Technology

UMUC is offering cybersecurity majors two new scholarships—one for undergraduates and the other for graduate-level students. The Cybersecurity Transfer Scholarship is available to undergraduate students who meet the following criteria: Applicants must have obtained an associate's degree or a minimum of 60 credits from a regionally accredited community or technical college. They must have a minimum cumulative 3.2 GPA. They must be pursuing a first bachelor's degree. The Graduate Cybersecurity Scholarship is available to new graduate students who have been admitted to the Cybersecurity degree program at UMUC, and are enrolled in at least 6 credit hours per semester.

To raise general cybersecurity awareness, UMUC has created a general education course on cyber security. In the first semester UMUC has about 300 enrollments, most from students in noncomputing fields.

Towson University (TU) has launched the School of Emerging Technology. The School will (1) promote interdisciplinary programs involving two or more academic areas, or involving TU personnel and external partners, that might otherwise have difficulty collaborating successfully; (2) provide resources such as administrative support, start-up "seed" funds, and space for such programs; and (3) highlight TU's interdisciplinary educational and research programs both within and outside of the institution. One of the first projects of the school was the development of a joint research project proposal to DoD in cloud computing security with an area firm.

Students attending BSU, TU, UMBC, UMCP and UMES as National Centers for Academic Excellence in Information Assurance are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. The distinction provides support for universities that promote and practice information assurance and cyber security programs, which are essential to securing the national information infrastructure.

3. Establish more partnerships among education and government and private industry and leverage the resources available.

UMUC, UMCP and UMBC working with industry and federal agencies. UMCP is working with corporate partners focused specifically on cybersecurity collaboration, including research cooperation, student engagement, education, and curriculum development. Partners include: Lockheed Martin, SAIC, Tenable, MIT Lincoln Laboratory, ManTech and Google. UMCP & Google Cybersecurity Seminar Series: forum for industry, academic, government thought leaders, facilitate discussions between experts in public and private sectors targeting innovative cybersecurity solutions from a comprehensive perspective.

UMUC is participating in the **National Initiative For Cybersecurity Education (NICE)** initiative at NIST, including the mapping of our degree programs to Federal Government and Industry and cyber job titles. (UMUC was the first university approached to do this)
UMUC has partnered with the Anne Arundel Workforce Development Corporation to offer their cyber security programs.

AT UMBC the Cyber Incubator@bwtech is a unique, innovative business incubation program that delivers business and technical support to early stage companies providing cybersecurity-related products and services. The incubator is located in a Class A office suite at the bwtech@UMBC Research Park, adjacent to the campus of the University of Maryland, Baltimore County (UMBC).

Cybersecurity Companies at bwtech@UMBC
Advantage Incubator/Northrop Grumman Cync Program. The Advantage Incubator applies bwtech's

successful business incubation framework to support companies working in the emerging field of cybersecurity. The incubator is ideally located for this work: It is minutes from BWI Airport and 10 miles from Fort Meade, home to the National Security Agency (NSA), U.S. Cyber Command and, later this year, the Defense Information Systems Agency. Cybersecurity companies at bwtech also have access to UMBC resources.

The Northrop Grumman Cync Program is a key part of the Advantage Incubator. It is an innovative program that allows companies to draw on UMBC's research expertise, bwtech's incubation experience and Northrop Grumman resources to develop technology that will secure and protect the computer hardware, software and networks vital to national defense. The goal is to "open the aperture" to the new tools that will be needed to detect, monitor and control cyber threats. Early stage companies from across the country are invited to apply to the program.

Northrop Grumman Cync Program companies:
Five Directions Five Directions is an early-stage company working to develop technology that would enable high-assurance file sharing via public or private clouds. Using a data-centric approach, Five Directions secures access through credentialing, encryption, and a robust audit trail. The company's founder, William Arbaugh, also started Komoku, a provider of advanced rootkit security detection solutions, which was acquired by Microsoft in 2008.
Rogue Networks Rogue Networks is working to develop BreachBox, a product that enables traffic monitoring, alerting, and the enforcement of flow policies on large enterprise networks. This early-stage company recently deployed BreachBox during a pilot study with the U.S. General Services Administration (GSA) to enforce traffic policies and contain activity based on internal identity use.

Other Advantage Incubator companies:
Calvert Systems Engineering, Inc. (CSE) CSE is a dynamic, woman-owned Engineering and Consulting Services firm with locations in Maryland and Nebraska. Services include software and systems engineering, configuration management, quality assurance, and program management. Specialties include C4ISR and signals processing custom applications development. CSE provides customers with full software development life-cycle support, including requirements analysis, software design and implementation, and formal testing using CMMI Level 3 equivalent processes and procedures.
Catomi Systems Catomi Systems is a new company providing high-level expertise in metrics, cost estimating/modeling, earned value management, financial/budget analysis, enterprise resources planning, financial systems design/implementation, and systems engineering (process mapping, simulation, and software requirements) to the Federal intelligence community, DoD, and other Federal agencies.
Cyber Map Cyber Map is creating an online map showing Maryland's cyber resources and facilitating networking between companies. The Cyber Hive, a Cyber Map program, will allow new and established companies from across the country to establish a presence in Maryland, giving them access to the region's cyber resources and opportunities.
Fearless Solutions Fearless Solutions is a minority owned business that serves a variety of Federal, state and local government clients as well as commercial sector clients. The company's core competencies include: visualization, Rapid Prototyping / Proof of Concept, Software Engineering / Web Application Development, Development Infrastructure Setup, Project and Program Management and Equipment procurement.
Intellibit Systems. LLC Intellibit Systems LLC. is a minority-owned, and veteran-owned business providing professional network data communications and information technology support services to government and commercial clients. They also offer professional information technology education and public outreach services.
Premier Management Corporation (PMC) Premier Management Corporation (PMC), an 8A, Service Disabled Veteran-Owned (SDV) small business founded in November 2004. The company provides consulting services to government agencies in the areas of financial operations and acquisitions, and recently established divisions focusing on cyber crimes and network security. While still offering financial consulting services, the Company's focus is shifting to developing technologies that detect vulnerabilities and attacks via the Internet in government computer networks. Current customers include NSA and the FBI.
Technology Security Associates Technology Security Associates (TSA), Service-Disabled Veteran-Owned Small Business, supports a wide-ranging group of Department of the Navy acquisition programs in the areas of technology and information security and international programs. TSA also supports several small

and large commercial clients in Information Security.

4. Strengthen research and support innovation and technology transfer in cyber security.

UMCP: Continuing to develop innovative research solutions to cyber security. UMCP faculty just received $1 million agreement with NIST for cyber-physical systems research to help NIST develop/deploy standards and test methods to support reliable performance of new smart systems.

The Maryland Cybersecurity Center (MC^2) at UMCP was created as an interdisciplinary research center, bringing together experts from engineering and computer science with colleagues from across campus in fields such as information sciences, business, public policy, social sciences and economics to address our nation's growing needs in cybersecurity. Maryland researchers will apply their expertise in wireless and network security, cryptography, secure software, cyber supply chain security, cybersecurity policy, multimedia forensics, and the economics of cybersecurity, offering an innovative, holistic approach to the cybersecurity threat. Maryland Cybersecurity Center (MC^2) is partnering with government and industry to provide educational programs to prepare the future cybersecurity workforce, and develop new, innovative technologies to defend against cybersecurity attacks.

The **(UMBC)** Center for Information Security and Assurance (CISA) promotes research, education, and sound internal practices in information security and assurance. CISA's Cyber Defense Lab provides an isolated network of workstations available to UMBC students and faculty for research projects and classroom exercises.

5. Expand the cyber security career pipeline through collaborations between the USM and Maryland's community colleges. As part of this coordination, adopt models to increase awareness and reduce impediments to obtaining a security clearance.

The USM initiated an Articulation Committee of public and private universities and community colleges to establish a foundation for statewide articulation in Cyber Security. This work is expected to be completed by May 2012.

- The Cyber Security Articulation Committee has met three times (5/3, 6/21, 9/13) since its initial organizational meeting (4/12).
- The following institutions have participated at various times:
- Bowie State University, Capitol College, FSU , Loyola, UB, UMCP, UMES, UMUC, Towson, AACC, CCBC, CSM, Frederick CC, Garrett CC, Hagerstown CC, Howard CC, PGCC, Montgomery College, with USM
- Four-year and two-year co-chairs have been selected.
- The charge to the committee is described in the memo sent to Intersegmental Chief Academic Officers (ICAO's) requesting that each provide two representatives to the Cyber Security Articulation group. Below is an excerpt from that memo.

  "…at the most recent ICAO meeting, the USM (under the auspices of the ongoing USM/MACC Articulation efforts) will convene a group to begin laying the foundation for statewide articulation in Cyber Security. The group will consist of members from USM institutions, Maryland community colleges and those private institutions who previously paid to participate in the USM/MACC Articulation project…USM seek names of faculty from your institutions to participate in a group to begin seriously examining the parameters of a statewide articulated program in Cyber Security."

The statewide articulation effort is focused upon statewide articulation from two-year institutions to four-year institutions.

- The committee discussed what constitutes a cyber security program for this work. The discussions revealed that there were four pathways/initiatives that existed:
    - Pathways built upon/connected to/currently articulated from existing 2-year AAS and/or AS related programs.
    - Pathways contained within an existing program such as Computer Science, Information Systems, or Information Technology
    - Initiatives that attempt to infuse cyber security outcomes across a program, programs, or courses throughout an entire institution
    - Pathways identified as Cyber security programs (named as such and are relatively new)

- The AAS pathway is the most developed/connected to/articulated, so identifying the cyber security outcomes for the first two years for 4-year programs that fit this pathway and student characteristics, will be the first emphasis of work.

    - The committee is currently collecting outcomes for the first two years from four-year and two-year schools. These outcomes are expected to be received and collated by December 2011. The Cyber Watch outcomes will be included in this set of outcomes. In Spring 2012, the committee will then add, modify, delete outcomes as needed to achieve a common set of critical outcomes to form the basis of a statewide articulation agreement for those schools pursuing programs consistent with these outcomes. This work is anticipated to be completed by May 31, 2012.

- The AAS pathways are more closely associated with those cyber security programs contained within an existing program such as Computer Science, Information Systems, or Information Technology. We have set up a joint articulation meeting with these committees (Computer Science, Information Systems, and Cyber Security) for November 1 to discuss how best to introduce the cyber security discussion/work into these deliberations.

UMCP hosted a one-week summer cyber camp for high school students, partnering with NSF's Cyber Watch and the Community College of Baltimore County.

STUDENT ACHIEVEMENTS

The University of Maryland team won the 6th annual CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition (**MA CCDC**) on Saturday, March 12, 2011

(03/17/2010) The Towson University student team won the mid-Atlantic Regional Cyber-Defense Competition

FORUMS, SPEAKER SERIES, CONFERENCES

UMBC: In support of the Governor's CYBERMARYLAND Initiative, UMBC co-founded the Maryland Cyber Challenge and Conference (MDC3) to encourage high school and college students to pursue careers and education through a statewide cyber-defense competition resulting in scholarship prizes. (October 21 -22, 2011 – Baltimore Convention Center)

Smart Grid Cyber Security Conference held at UMBC on February 15, hosted by the UMBC Computer Science and Electrical Engineering Department and Maryland Clean Energy Technology Incubator.

Charles Croom, of Lockheed Martin spoke about "The State of Cyber Security 2011" at the UMBC Visionaries in IT Forum, February 23, 2011

UMCP: *Maryland Cybersecurity Center, The Google and University of Maryland Cybersecurity Seminar Series*.

"Looking Before You Leap: The Argument for Data-Driven Security" Stefan Savage, Professor, University of California, San Diego, September 1, 2011

"Can We Make the Internet Safer?" Vint Cerf, Chief Internet Evangelist, Google
April 7, 2011

"Intrusion Detection and Network Security Perspectives From A Veteran", Martin Roesch, Chief Technology Officer, Sourcefire, April 21, 2011 Center for International and Security Studies at Maryland – School of Public Policy.

"Cybersecurity: The Evolving Threat", Roger Cressey, President, Good Harbor Consulting LLC, Oct 21, 2010

"Cyber Attack: The Opaque Dimension of Cyber Security", Herbert Lin, Chief Scientist, Computer Science and Telecommunications Board, The National Academies, Oct 01, 2009.

.