BOARD OF REGENTS

SUMMARY OF ITEM FOR ACTION
INFORMATION OR DISCUSSION

TOPIC: USM Cyber Security Task Force Recommendations – Progress Report (information item)

COMMITTEE: Economic Development and Technology Commercialization

DATE OF COMMITTEE MEETING: January 24, 2013

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 January 2013 progress report on the recommendations of the USM Cyber Security Task Force.

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

FISCAL IMPACT: This item is for information purposes.

CHANCELLOR'S RECOMMENDATION This item is for information purposes.

COMMITTEE RECOMMENDATION: DATE:

BOARD ACTION: DATE:

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

University System of Maryland Cyber Security Task Force
Recommendations Progress Report
January 11, 2013

The USM Cyber Security Task Force made a number of actionable and achievable recommendations. Activities, programs and initiatives now taking place to respond to these recommendations are listed below.

1. Conduct a comprehensive and scientific survey of employer needs.

The USM was planning on working with the Governor's Workforce Investment Board to conduct this survey however we have been fortunate to benefit from the results of a Cyber Security Jobs research project just completed by The Cyber Technology & Innovation Center, the Abell Foundation, Cyber Maryland, CyberPoint International and Weiz and Weissel Communications. This report was completed on December 17, 2012 and contains the most recent and applicable data. A copy of the full report is available. Below are some key findings and data points that will be used as the USM and our institutions continue to address the needs of students, workforce, private sector and government agencies. This report found that 1,828 entities in Maryland have 19,413 cyber security related job openings currently. This is consistent with the projections of over 30,000 cyber jobs in Maryland that will be open during this current decade. This report also identified the unique job opening titles as well as skill set and educational degree requirements. The specific job title openings in order of need are listed below:

Software Engineer	Cyber Security Engineer
Systems Engineer	Software Developer
Systems Administrator	Network Analyst
Network Engineer	Computer Security
Java Developer	Information Technology
Database Administrator	Cloud Administrator

Education Requirements	Work Experience
Bachelor's Degree – 76%	10-15 Years – 33%
High School Diploma – 17%	2-5 Years – 31%
Associate's Degree – 3%	0-2 Years – 29%
Master's Degree – 3%	7-10 Years – 4%
Doctorate Degree – 1%	5-7 Years – 3%

Maryland leads the nation in the number of Colleges and Universities Certified in Cyber Security by the National Security Agency (NSA) with 15 meeting this criteria. This independent report found:
"Job opportunities for STEM-related prospects are prevalent at all levels of education and experience. To address these urgent needs; Maryland higher education institutions are well positioned and lead the nation in programs certified by the NSA in Cyber Security. The programs with this unique distinction offer technical and professional certifications, undergraduate and advanced degrees, and cutting-edge research and training opportunities. Partnerships exist with government agencies to introduce cyber security education to K-12 students as well."

The USM and it's institutions will continue to work with state and federal agencies and the private sector to continue to monitor and meet the workforce needs in cyber security.

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 System of Maryland (USM)

Between 2011 and 2012, the USM has approved seven new certificates and degree programs in cyber security, information assurance, and cyber forensics. In addition, UMUC offers cyber security programs at the several of the regional higher educations in Maryland, as well as on-line.

University of Maryland College Park (UMCP)

UMCP last year offered or established several new undergraduate courses:

- (Spring 2012) **CMSC 498B Secure Maryland**, course on penetration testing of on-line systems; found hundreds of vulnerabilities in live, UMCP on-line services. http://www.cs.umd.edu/~mwh/securemd/CMSC498B__Secure_Maryland/Home.html To be offered again in the Spring of 2013.
- (Spring 2012) **CCJS 418 Cyber crime**, studied cyber criminals from a criminal justice point of view (e.g., contrasting with non-cyber criminals)
- (Spring 2012) **PUAF 388I: Special Topics in Public Policy: Intelligence as a National Security Instrument, The US Experience**, examined national security generally, with a liberal set of course topics covering cybersecurity
- (Fall 2012) **CMSC 498L Cybersecurity Lab**, involving five professors in computer science and engineering presenting a lab-oriented view of a wide range of security topics, from software security to intrusion detection to cryptography to hardware security http://www.cs.umd.edu/class/fall2012/cmsc498L/
- (Fall 2012) **HONR378N Research in Science and Public Policy for the U.S. National Security Agency**, honors course in which students studied possible solutions to NSA problem sets, taking a multidisciplinary perspective http://universityhonors.umd.edu/378N1208.php
- (Fall 2012) **CMSC 498M Revealing Stealth Malware**, to be taught during the 2013 Winter term by Xeno Kovah of the MITRE corporation. http://www.cs.umd.edu/class/winter2013/cmsc389m/

UMCP has also established or begun several new cybersecurity-specific degree programs and concentrations during 2012:

- Professional Masters and Certificate in Cybersecurity, established Fall 2011 and started Fall 2012 http://advancedengineering.umd.edu/programs/cybersecurity
- Graduate Certificate in Cybersecurity Leadership, established Spring 2012 and to start Spring 2013 https://www.rhsmith.umd.edu/cybersecurity/
- Advanced Cybersecurity Experience for Students (ACES), the nation's first undergraduate honors program in Cybersecurity, established Spring 2012 and to start Fall 2013. http://www.aces.umd.edu/
- Computer Science has approved a cybersecurity concentration for computer science degrees. This concentration was developed in consultation with the NSA, and approved Spring 2012, to be available on diplomas Fall 2013. Electrical and Computer Engineering also is working on a concentration. http://www.cyber.umd.edu/education/concentrations

The number of undergraduate majors in computer science, the major with the most training in cybersecurity offered at UMCP, continues to rise. In particular, in the Fall of 2010 there were 972 Computer Science majors; in Fall 2011 there were 1176 majors; and in the Fall of 2012 there were 1252 majors. There are similarly high numbers of computer engineering majors.

Outside of courses, UMCP cybersecurity education includes outreach events and experience-driven clubs:

- Fall 2012: Cool Cybersecurity Careers for Girls event, attended by 350 middle-school girls, http://www.cyber.umd.edu/education/cool-careers
- The UMCP cybersecurity club (http://csec.umiacs.umd.edu/) is a student-run and organized club (with faculty advisors) that hosts speakers, takes field trips to local companies, and trains for competitions. The club's "A team" has a history of successful competition results; e.g., it placed first in the MDC3 competition in Fall 2012. Consists of about 60 active members, and has a mailing list of over 600.

Bowie State University (BSU)

- Established a cybersecurity lab in the Department of Computer Science
- Developed an undergraduate security track in cybersecurity under the Computer Technology program
- Established a Master's degree program in Management Information Systems with a concentration

in cybersecurity
- Over ten peer-reviewed publications in cybersecurity research
- Established an online cyber security laboratory in the Department of Management Information Systems
- BSU designated a Center of Academic Excellence in Information Assurance Education (CAE/IAE) by DHS and NSA on June 14, 2011
- Established a cybersecurity team and competed in several competitions

Frostburg State University (FSU)

The department of Computer Science and Information Technologies initiated a new BS in Secure Computing and Information Assurance degree commencing Fall 2012. FSU already has an enrollment of 20 students with enrollment projection of 80 students within 3 years. Graduates will have the skills necessary to satisfy security needs in government and industry.

University of Baltimore (UB)

- UB's School of Information Arts and Technology has a new cyber security track that was developed as part of its 4-year undergraduate Applied Information Technology degree program.
- Additionally, UB will have a new degree on cyber crime, pending review and approval by USM and MHEC of its proposal.

University of Maryland University College (UMUC)

UMUC has launched an MS/Digital Forensics and Cyber Investigation. Fall 2012 was the first semester. This is in addition to the degrees already captured in the May 2011 USM Cybersecurity Task Force Report, including the MS/Cybersecurity, MS/Cybersecurity Policy, BS/Cybersecurity and other closely related degree programs identified in the Report.

University of Maryland Baltimore County (UMBC)

- New Masters in Professional Studies (MPS) program in Cybersecurity jointly offered between CSEE Department and Division of Professional Studies. This program has grown very quickly, and now enrolls over 140 students. http://www.umbc.edu/cyber/
- Expansion of UMBC MPS in Cybersecurity program to Universities at Shady Grove approved to begin in Fall 2013.
- CDP Cohort students from NSA taking graduate courses at UMBC.
- New (to be launched in Fall 2013) CyberScholars program, which will be intended for CS, CE, and IS majors initially, and to be expanded to other majors. These scholars will get research experience and industry/government mentorship from freshmen year. The program is initially funded by a $1 Million grant from Northrop Grumman. http://cybersecurity.umbc.edu/cyberscholars/
- New $2.5 Million grant from NSF to support Scholarships for Service cybersecurity scholars at BS, MS, and PhD level.
- UMBC Training Centers (Columbia, MD) established its Center for Cybersecurity Training in 2012 to provide non-credit professional technical training and certification programs in cybersecurity.
- Continuing Progress in converting the CSEE "Dean's Letter" in cybersecurity to a certificate.
- The number of CS and CE majors has increased significantly, and the department is continuing to make sure that as many as possible can take our offerings in Cybersecurity area.
- Initial Discussions with DC3 on Cyber Forensics program
- Continuing stream of Graduate students working in Cybersecurity area in CS, CE, EE, and IS programs
- UMBC co-founder of Maryland Cyber Challenge to encourage HS and college students to pursue STEM & cybersecurity educational paths. Challenge is enhanced by significant prize monies contributed by NSA to support students' higher education and training in these fields.

Bowie State University (BSU)

- Established an experiential, learning, cybersecurity capstone course for the existing undergraduate cyber security track in the Department of Computer Science's technology program through a $20,000 DoD grant (2011 – 2012).

- Course modules are being developed for the Computer Science senior capstone course by incorporating security-related topics. We have created project modules for face-recognition based smartphone authentication system, encryption and decryption of the file system in Android environment, etc.

Towson University (TU)

In discussion with NSA staff, they suggested the development of course work in malware analysis and reverse engineering for our undergraduate computer science track in computer security. TU consulted with experts both at NSA and at ManTech International who both offer similar courses for their employees, and developed two courses to address this area, one in advanced programming and assembly language, and a second in reverse engineering and malware analysis. These courses will be offered for the first time in Fall 2013.

In the Applied Information Technology Masters program, TU has developed a new course in Mobile Device Forensics. The development of this course was supported by a grant from the Department of Defense that allowed us to purchase the necessary equipment and hardware.

The Security Injections @ Towson project (www.towson.edu/securityinjections) is an NSF funded project ($850K), which integrates security in the undergraduate computer science curriculum and includes and training and extensive dissemination effort. Towson faculty works with faculty from Bowie State University and three community colleges: AACC, CCBC, and Harford Community College to: 1) Increase number of security aware students 2) Increase students' security awareness 3) Increase students' ability to apply secure coding principles and 4) Increase faculty security awareness. [This is relevant for Recommendation #5].

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

University System of Maryland (USM)

In 2012, the Business Higher Education Forum (BHEF) of which Chancellor Kirwan is the Chairman, announced twelve regional projects in which member companies and universities collaborate in key fields important to national competitiveness and security, such as cyber security, large-data analytics, water and materials science, and information technology.

Cybersecurity as a Focus Area. Among the fields identified for the BHEF regional projects, cybersecurity has emerged as one of particularly high need by government, industry and higher education partners. To date, four BHEF member institutions—Cal Poly, Miami Dade College, San Jose State University, and the University System of Maryland (with Bowie State University, Towson University, University of Maryland Baltimore County [UMBC], and University of Maryland College Park [UMD])—have opted to focus on cybersecurity, each from a different perspective. With support from the Alfred P. Sloan Foundation, BHEF conducted a planning exercise to develop a framework for industry-higher education collaboration around undergraduate cybersecurity education in Maryland which led to a major investment by Northrop Grumman in an innovative undergraduate residential honors program in cybersecurity, known as Advanced Cybersecurity Experience for Students (ACES), at UMD, due to open in fall 2013. Northrop Grumman subsequently awarded another substantial grant to replicate this model at UMBC. In October 2012, BHEF received a major implementation grant from the Sloan Foundation to expand its partnership with the USM to learn from the ACES program at UMD and expand undergraduate cyber with new projects at Bowie State University, Towson University, and UMBC through innovative collaborations of higher education, industry, and government. Driving this project will be the USM Undergraduate Cybersecurity Network, comprised of regional industry, higher education, and government leaders concerned with the future of the Maryland cyber workforce.

University of Maryland College Park (UMCP)

Many UMCP education activities described above involve corporate and government partners, to enhance and diversify the educational content:

- SAIC and Northrup Grumman guest lecturers in CMSC 498B
- Instructor for CMSC 498M from MITRE
- HONR378N in close collaboration with the NSA (researching NSA-provided problem sets)
- Northrup Grumman sponsored the ACES program ($1.1M gift) and will provide advisors and internship positions for students
- Cool careers event co-organized with CyberWatch (http://www.cyberwatchcenter.org/) K-12 Division, and sponsored by Google and Educational Technology Policy, Research, & Outreach
- Drs. Maimon and Cukier research cybercriminal behavior with support from the non-profit SANS Institute

UMCP has several research partnerships with government centers:

- The University of Maryland Institute for Advanced Computer Studies (UMIACS) has a longstanding relationship with the NSA's Laboratory of Telecommunications Sciences (LTS) http://www.ltsnet.net/. The latter funds and provides research collaborators for Maryland cybersecurity-related research projects.
- The Center for Advanced Study of Language (CASL) is a UARC at UMCP with ties to the NSA. http://www.casl.umd.edu/
- National Consortium for the Study of Terrorism and Responses to Terrorism (START) partners with the Federal government, considering cyber-related vectors of terrorism. http://www.start.umd.edu/start/
- The Center for Public Policy and Private Enterprise (CPPPE) partners with government and industry to discuss matters of public policy, including approaches to cybersecurity and responses to cyber attacks. http://www.cpppe.umd.edu/

UMCP's Maryland Cybersecurity Center (MC2), established in December 2010, is the nexus of many government/industry collaborative activities: http://www.cyber.umd.edu/

- MC2 has an active corporate partners program http://www.cyber.umd.edu/partners
    - Large partners: SAIC, Lockheed Martin, Google, ManTech, Northrop Grumman
    - Small partners: MIT Lincoln Labs, Tenable, Future Skies, Lunarline, SuprTek, Mar Inc., AdvanTech, Cyberpoint LLC, Sourcefire
    - Several partners in regular attendance at MC2 bi-monthly internal tech. seminars
- MC2 faculty have had numerous corporate interactions
    - (UMCP faculty visited company site) SAIC, Lockheed Martin, Google, CyberPoint, SuprTek, MAR Inc., Boeing, ManTech, Symantec
    - (hosted at UMCP) ARINC, AT&T, NGC, IBM, Siemens, Battelle, Team Cymru, CTIA, Neo Prime
- MC2 hosted its first annual Symposium (Spring 2012) http://www.umiacs.umd.edu/mc2symposium/
    - Keynotes by industry and academics
    - 150 attendees from local industry, government, academia
    - 12 corporate tables (largely from MC2 corporate partners)
    - Panels and welcomes from government personnel (including Ruppersberger)
    - Tech talks from MC2 professors
- Google sponsors MC2's Cybersecurity Seminars http://www.cyber.umd.edu/events/google-seminars
    - 6 seminars offered during 2012 featuring external speakers: three from industry, two from government, one from academia
    - Attendees a mix of academia, government, industry (typically ~100 per seminar)
- MC2 has an External Advisory Board http://www.cyber.umd.edu/about/advisory-board
    - Comprised of 11 industry leaders
    - First meeting held October 2012
- MC2 Director Michael Hicks is the point of contact for UMCP as an NSA Center of Academic Excellence (in Research) http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml
    - Meeting held in December 2012 established plans to expand UMCP certification to include information assurance education (IAE) and potentially also operations (OPS).
- MC2 Director, Prof. Michael Hicks, is a member of the State of Maryland's Cyber Task Force (run out of the office of business and economic development (DBED))
- During 2012, MC2 had a partnership with the Napier Meridian consultancy, which published a monthly cybersecurity newsletter with UK and US government readership.

There are several industry/government partnerships initiated by the business school:

- Sandor Boyson collaborates with NIST on determining ways to secure the IT supply chain (cf. http://www.rhsmith.umd.edu/scmc/)
- Professors Larry Gordon and Martin Loeb sponsor an annual symposium, held in January, on cybersecurity topics, inviting leaders from the business and legal community. http://www.rhsmith.umd.edu/faculty/lgordon/Forum%20on%20Financial%20Information%20Systems%20and%20Cybersecurity.htm

UMCP representatives met with representatives from University of Maryland, University College (UMUC) during the Fall of 2012 to work out an articulation of strengths, to each help the other identify the best student constituencies and advertise accordingly on their web sites. Discussions are in progress.

MC2 continues to explore research collaboration opportunities with various agencies in the US Government. This has included: NIST, NSA, CIA, and the FBI, among others.

Bowie State University (BSU)

- Received $1M equipment donation from Cisco Inc. to establish a cybersecurity instructional lab.
- BSU was awarded over $300,000 in federal grants to enhance cybersecurity research and education.
- BSU was awarded $500,000 DoD grant for network security research and cybersecurity education.
- Working with DoE's National Nuclear Security Administration (NNSA) to facilitate cybersecurity training of faculty and students at federal labs, and to help to close the gap between cybersecurity education and the needs of government and industry.

Frostburg State University (FSU)

A future goal is to apply for membership in National Center of Academic Excellence in IA education (CAE/IA) – sponsored by NSA and Homeland Security. IBM has a need for security professionals for employment at the local division. FSU is an IBM-sponsored member of the SAP University Alliance Program.

University of Baltimore (UB)

With Senator Mikulski's support, the University of Baltimore received a $150,000 cyber security education grant from the FY 2012 appropriation of the Dept. of Homeland Security to launch Maryland's first and only university-led Integrated Cybersecurity Education Communities (ICEC) program. These grant funds allow UB to be a participant in the Shreveport/Bossier City, Louisiana Cyber Innovation Center's demonstration project—a professional development model known as Cyber Discovery that works to stimulate interest among high school students for cyber and STEM-related fields. UB hosted teacher workshops and a successful residential summer camp for students from several area high schools as part of its Cyber Discovery programming.

University of Maryland University College (UMUC)

UMUC is part of the human capital development strategies in cyber with the following firms with which it has education partnership agreements: Boeing, Booz Allen Hamilton, CACI, ManTech, Northrop Grumman and SAIC.

University of Maryland Baltimore County (UMBC)

UMBC takes an integrated approach to work with companies and agencies, working across hiring/recruitment, research, and economic development initiatives. The "case management" approach helps us identify key partners, develop priorities, and collaborate on execution in a way that helps us meet and exceed expectations. UMBC's Center for Cybersecurity was established in 2012 to streamline and leverage UMBC's institutional capabilities to meet the challenges and critical State needs in the area of Cybersecurity. It acts as a single point of contact with external partners. Specific recent partnership examples include

- IRAD funding from industrial partners to support research, such as Northrop Grumman and the Johns Hopkins Applied Physics Lab
- Joint proposals being written to federal agencies with companies (e.g. DARPA Plan X collaboration between Northrop Grumman and UMBC)

- Novel programs like CYNC,a collaboration between UMBC and Northrop Gruman and UMBC) which supports early stage companies in the cybersecurity areas.
- Philanthropic support from companies to help in setting up labs, e.g. BAE support for CS Lab for freshmen, BAE and Northrop support for a Cyber Lab.
- Close collaboration between UMBC and NSA to raise profile of cyber related jobs, leading to increased hires. Similar collaborations between UMBC and several area companies
- Significant NSA participation in CSEE colloquium series to foster additional collaboration
- The Career center is aggressively encouraging our cyber-business partners to either start or expand their internship programs so that more students will graduate with the critical job knowledge and clearances required of this industry.

Towson University (TU)

A Research and Education Partnership Agreement has been signed between the Army Research Laboratory (ARL) and Towson. This partnership is authorized under 10 U.S.C. Section 2194 (authorizes Directors of Defense laboratories to enter into educational partnership agreements to encourage and enhance study in scientific disciplines) and 10 U.S.C. Section 2195 (authorizes the establishment of education programs for undergraduate and graduate education). The agreement specifically mentions that the ARL agrees to involve TU students in research and other activities through internships, cooperative education programs, visiting lectures, and site visits.

Towson University faculty have participated in a number of funded research projects with area companied and government agencies; examples include

- Altoona Regional Health Systems, *Design and Evaluation of a Health Care Information System ($234K)*
- Army Research Laboratories, *A Distributed Host-Based Intrusion Detection Framework for Military Network Operation* ($198K)
- National Institute of Standards and Technology, Smart Grid Priority Action Plans: Network Assessments for Smart Grid Applications ($181K)
- Department of Defense, *Effective Routing Algorithms for IP-based Satellite Networks* ($46K)
- Department of Defense, *A Network Sensor-Based Defense Framework for Active Network* ($40K)

(Also relevant for Recomendation #4).

Towson University undergraduate and graduate students have worked directly with a number of local companies and organizations on security related projects; examples include:

- Brian Coats (Doctoral): Secure Electronic Health Record Exchange: Achieving the Meaningful Use Objective with Federal Government HealthCare Organization (Fall 2011- present)
- Jason Cohen (Doctoral): Incorporating Hardware Trust Mechanisms in Apache Hadoop (HP Research) (Spring 2012 – present)
- Imoh Noah (Undergraduate): A Secure Framework for providing privacy aware differentiated services in Electronic Health Records with Federal Government HealthCare Organization (Fall 2012 – present)
- Clinton Edmonds (Graduate): Network Security Assessment for People Encouraging People, Inc. (Completed in December 2011)

Towson University has been working with the Mid-Atlantic CIO Forum for 10 years to advance excellence in the field of information technology. The CIO Forum has offered scholarships to TU students studying business, economics, and computer information sciences since 2006, including $15,000 in scholarships for the spring 2013 academic term. These scholarships help the top TU students in these fields build a foundation for their careers by allowing them to further their education and cultivate their skills. Recipients also have the opportunity to participate in Forum meetings and interact with information technology executives from across the Mid-Atlantic region.

Bowie State University (BSU)

- $453,000 grant for one year from DoE’s National Nuclear Security Administration (NNSA) (September 1, 2012 through August 31, 2012) to facilitate cybersecurity training of faculty and students at Sandia National Lab for a consortium of five Historically Black Colleges and Universities (HBCUs) that includes Bowie State University (BSU), Norfolk State University (lead), University of the Virgin Islands, North Carolina A&T and Voorhees College. This project aims to help to close the gap between cybersecurity education and the needs of government and industry.

- $499,000 grant was acquired from DoD for conducting research on authentication protocols for wireless ad hoc networks and for incorporating research into education.

Salisbury University (SU)

SU has developed an academic program in collaboration with Tallinn University of Technology (TUT) and the University of Tartu (UT) in Estonia. SU chose to leverage their relationships with these institutions because of their sister state relationship with Estonia and their existing and highly regarded MS program in Cyber Security which is delivered collaboratively between TUT and UT and in English. UT, established in 1632, is one of the leading higher educational institutions in Eastern Europe. TUT is Estonia's flagship for technical education and internationally recognized for its research and tech-related programs. Salisbury University faculty and administrators travelled to Estonia this June to discuss the curriculum and articulation agreement for a proposed 3+2 program between SU and TUT/UT. SU has also visited staff at the U.S. Embassy in Tallinn, leadership of Skype (headquartered on the TUT campus), and NATO's CCDCoE to develop a framework for the initiative including internships at the CCDCoE. The timing of the visit coincided with CyCon, the annual international conference of the CCDCoE, and SU had the opportunity to meet with Cyber professionals from MITRE (www.mitre.org) to talk about the program.

The program will allow SU students majoring in Computer Science, Mathematics, or Information Systems to pursue a Master's degree in Cyber Security at TUT/UT through a unique 3+2 program in which students take three years of study at SU and then enroll at TUT/UT as a 'visiting student' for one year. During Year 4, students will pay standard SU tuition and fees and SU will pay TUT/UT on behalf of the student. This will allow SU students who receive financial aid and scholarships to continue receiving this support while completing their undergraduate degrees. SU intends to send four to six students per year in this proposed program starting Fall 2013; program directors at TUT and UT state that they have the capacity to accept this number of additional students. Further, SU hopes to create a similar program for students interested in pursuing a MS in Software Engineering at UT, either through a 3+2 program or preparation for standard post-graduate study (i.e., completing degree requirements at SU and then going to Tartu for graduate school).

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

University of Maryland College Park (UMCP)

UMCP is highly ranked in the core research areas that include cybersecurity. In particular, it's Computer Science Department is ranked 14th in the USA by US News and World Report (last ranking in 2010), and 16th in the World by the Academic Ranking of Worldwide Universities (ARWU). UMCP is one of only six Universities worldwide to be ranked in the top 25 in each of Computer Science, Economics, Engineering, Natural Sciences and Mathematics, Physics, and Social Sciences, all areas which contribute expertise to the cybersecurity problem.

UMCP's MC2 comprises 26 core faculty across campus---in computer science, engineering, public policy, business, and criminology (among others)---actively engaged in cybersecurity research, with many more faculty in supporting roles. See our research brochure for a discussion of research that is ongoing.
http://www.cyber.umd.edu/sites/default/files/documents/2012-MC2-Research-Brochure6final.pdf

In addition to millions of dollars of ongoing funding, there were several new grants in 2012 (among others):

- Ankur Srivastava (ECE), National Science Foundation grant: *PI: Physically Unclonable Function (PUF) Enhancements Via Lithography and Design Partnership*, $500K over three years
- David Maimon (PI), Michel Cukier (Co-PI), Gary LaFree (Co-PI), Anthony Lemieux (Co-PI), National Science Foundation grant: *SBES TWC: Phase: Small: Protecting the Bazaar: The Ecology of Cybersecurity in Weakly Fortified Networks*, $647,804, 09/01/2012 – 08/31/2015
- Larry Gordon, Bill Lucyshyn, and Martin Loeb (co-PIs), DHS S&T grant on cybersecurity economics for $667,000 over two years
- Contract between UMIACS and the LTS for $1.5M over 1 year, with renewals possible for 2 more

years, for 10 projects involving 15 PIs

MC2, and UMCP generally, is a team member for SAIC's SSES NexGen $7B contract with the DOD

Maryland, via MC2, has made, and aims to make, new hires in cybersecurity:

- Elaine Shi was hired in July 2012 as an assistant professor in Computer Science http://www.cyber.umd.edu/faculty/shi
- Open searches for four positions were initiated in the Fall of 2012 (two in Electrical and Computer Engineering, one in Computer Science, and one for the MC2 Director position)

Non-disclosure agreements (NDAs) signed with Symantec corporation and Team Cymru, with collaborative projects in preparation

NSF Research Experience for Undergraduates (REU) 2012 site http://www.cyber.umd.edu/education/reu

Frostburg State University (FSU)

FSU graduate students in the master's program work with faculty on cyber security research. FSU has a history of engaging in successful MIPs-sponsored research and are working with regional companies to develop additional projects.

University of Maryland Baltimore County (UMBC)

- Significant funded research in cybersecurity area. Recent examples are new grants in the Cybersecurity area, such as the NSF SaTC program grant on "Policy Compliant Integration of Linked Data", LTS grant for Social Media Analytics to detect subterfuge, NIST grant for work in Cloud /Big Data Security Policies. These grants lead to student support, publications, and technology disclosures.
- New startup companies in the BWTech Cyber Incubator which interact with UMBC students and faculty.

Towson University (TU)

In addition to research with our corporate and government partners, Towson University faculty continue to work to develop improved ways to teach cyber security. Besides the security injections project described above in #2, Towson faculty have worked on funded projects to develop a virtual laboratory for teaching cyber security (DoD, $61K) and to replicate our very successful capstone course in cyber security at Bowie State University (DoD, $20K).

Bowie State University (BSU)

- $70,000 DoD grant for one year for cybersecurity research, K-12 outreach, and to establish: (1) a mobile security and forensics laboratory, (2) a cloud computing laboratory, and (3) a network security research laboratory at BSU.
- $249, 901 DHS Scientific Leadership Award for "Developing Homeland Security Expertise to Support Emergency Evacuation Research"

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.

University System of Maryland (USM)

Working from the draft standards for *Computer Science Curricula 2013 (CSC 2013)*, *Joint Task Force on Computing Curricula, Association for Computing Machinery, IEEE-Computer Society,* the USM/Maryland Community College Cyber Security faculty work group has established common core cyber security topics and outcomes to be embedded in the first two computer science courses offered by both two-year and four-year institutions. As soon as there is national adoption of the CSC 2013 standards (expected by summer 2013), the institutions will be able to finalize the articulation across the segments. In addition, the work group is working to establish "concentrations" in Computer Science programs that focus on cyber security/information assurance, exploring new models and pathways to transition Associate of Applied Science students into information technology programs. The work plan also includes the establishment of a web-based tool to provide information on Cyber Security workforce needs and academic pathways.

University of Maryland College Park (UMCP)

UMCP professors Michel Cukier and James Purtilo are members of the USM Cyber Articulation Committee, which is working to create the pathways for students from community colleges to the 4 year instituions.

Frostburg State University (FSU)

FSU has collaborated with Garrett Community College for an articulation with their cyber security program. We have been in contact with Baltimore Community College last year and plan to establish an articulation program with them. Hagerstown Community College is seeking approval of a cyber security program this year. FSU will work with HCC on articulation as well. Finally, FSU plans to develop an articulation programs in cyber security with Anne Arundel community College and Frederick Community College.

University of Maryland University College (UMUC)

UMUC has articulations with the following eight Maryland Community Colleges. All of the associate's programs identified are articulated to UMUC's BS in Cybersecurity.

Community College	Community College Program
Anne Arundel Community College	Information Assurance and Cybersecurity
Carroll Community College	Computer Information Systems
Chesapeake College	Computer Information Security
College of Southern Maryland	Computer Information Security
Hagerstown Community College	Cybersecurity
Hartford Community College	Information Assurance and Cybersecurity
Howard Community College	Network Security
Montgomery College	Cybersecurity

University of Maryland Baltimore County (UMBC)

- New Cyberscholars program will focus on such activities in the freshman year and beyond. This will involve seminars and one/one mentoring.
- Attempt to obtain support to diffuse this across disciplines – a large number of students in CS/CE and IS, and increasingly in other disciplines, will be eligible for jobs that require clearance. We are seeking external funding to create a security awareness course across majors.
- We are encouraging students to do internships that lead to clearance.
- Working with partners to see how a "pre-clearance" type process can be set up for students early on
- General STEM transfer issues (of which cybersecurity is a part) being worked on supported by a Gates Foundation grant to UMBC, in collaboration with CCBC, Howard Community College, AACC, and Montgomery CC.

Towson University (TU)

Towson University was awarded $2.1M from the National Science Foundation as part of their Scholarship for Service (SFS) program. This money will go to scholarships for students in cyber security who agree to work for the federal government for a period of time after graduation.

SPLASH@ Towson (www.towson.edu/splash) is a Secure Programming Logic course aimed at Seniors in High School. In fall 2012, the course was piloted for 13 high school girls. This one semester course was offered online and included videotaped sessions, online notes and assignments, proctored exams and the security injection modules from the Security Injections @ Towson project to ensure that students are introduced to important secure coding concepts. Students received four credits upon successful completion. This project was funded in part by the U.S. Department of Defense.

The Department of Computer and Information Sciences at Towson University, along with ETPRO, held an Intermediate CyberSTEM Camp on July 23, 2012-August 3, 2012. There were 17 high school students who attended and represented several county high schools, private high schools, and several public high school districts. Ten Towson faculty participated by teaching sessions and assisting with financial support via funded grants. The 2012 Intermediate CyberSTEM camp at Towson University was designed to fulfill three goals. 1) Expose students to college level instruction in diverse cyber fields; 2) Provide hands-on experiences with cyber technologies; and, 3) Promote a university education. Topics and activities included: Mobile Apps, GIS systems, building honeypots, Robotics; programming languages (i.e., Scratch, Python, JAVA, Wireshark), applying cybersecurity (i.e., System Vulnerability Assessment, Digital Forensics) and cyberethics topics (i.e., Ethical issues involving Computer and Internet Crime, Intellectual Property, Software Development, Social Networking, etc.). Additionally, Computer Science Security track undergraduate students conducted demonstrations and presentations on cyber defense activities.

Bowie State University (BSU)

- BSU is a participant in the USM Cyber Security Articulation Committee, whose aim includes seamless curricula alignment of cyber security programs with community colleges.
- BSU was awarded a $70,000 DoD grant for one year for cybersecurity research, K-12 outreach, and to establish: (1) a mobile security and forensics laboratory, (2) a cloud computing laboratory, and (3) a network security research laboratory.

Conclusion

The USM convened a Cyber Security Task Force in November 2010 and brought together, technology business leaders, university experts, federal and state agency stakeholders, to access the USM cyber security capacity, inventories, needs and workforce demands. In May 2011 the Task Force issued a report along with Governor O'Malley, U.S. Senator Barbara Mikulski and Congressman Dutch Ruppersberger. The report contained five actionable recommendations. The progress report above demonstrates the significant accomplishments and progress made on those recommendations to date. The USM institutions are fully engaged in the areas related to cyber security workforce training and cyber research. The State of Maryland, the USM, and the rich assets of the public and private sector are on the forefront of cyber and are the catalyst for Maryland being the epicenter of Cyber Security for our nation. The USM and it's institutions are committed to continue in this higher education leadership role and will continue to work with private sector employers, state and federal agencies to ensure that USM is doing everything possible to meet the growing and critical cyber security workforce demands.