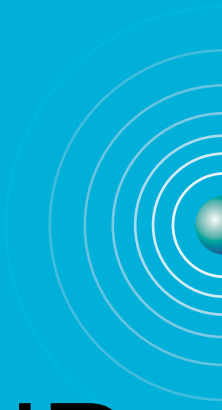
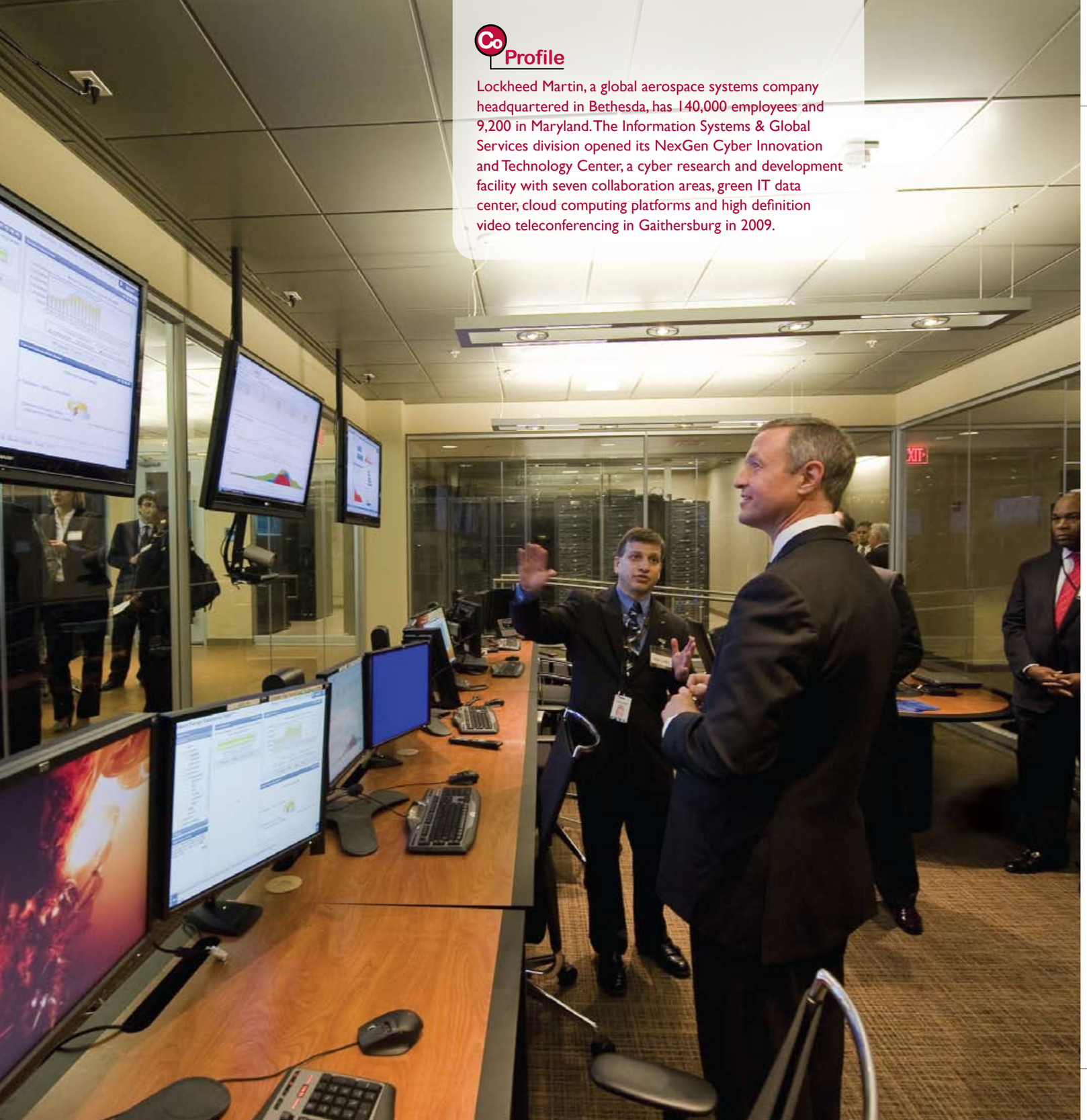


CYBERMARYLAND

Epicenter for Information Security & Innovation • Epicenter for Information Security & Innovation • Epicenter for Information Security & Innovation

A Report from the Maryland Department of Business & Economic Development

Martin O'Malley, Governor



Profile

Lockheed Martin, a global aerospace systems company headquartered in Bethesda, has 140,000 employees and 9,200 in Maryland. The Information Systems & Global Services division opened its NexGen Cyber Innovation and Technology Center, a cyber research and development facility with seven collaboration areas, green IT data center, cloud computing platforms and high definition video teleconferencing in Gaithersburg in 2009.

CONTENTS

< < < Governor O'Malley tours Lockheed Martin's new NexGen Cyber Innovation and Technology Center.

A Letter from the Governor

Answering the President's Call to Defend and Protect Our Nation's Information Networks

President Barack Obama recently pledged to make securing the country's most vital computer networks a top economic and national security priority. In doing so, he called for greater leadership and collaboration to improve the safety of information networks that power the government and the U.S. economy. Maryland – with its vast resources of federal facilities, academic institutions, industry strengths and intellectual capital – is answering the President's call to action.

Already a national epicenter of federal cyber security activities, Maryland is home to: the National Security Agency, the Intelligence Advanced Research Projects Activity, the National Institute of Standards and Technology and Defense Information Systems Agency headquarters beginning in 2010. Coupled with the expected location of the U.S. Cyber Command headquarters this year and the pending Department of Defense expansions of the intelligence and communications responsibilities at Fort Meade and at Aberdeen Proving Ground, Maryland is the base for our nation's efforts to defend and protect U.S. information networks.

Maryland resources make us a national leader in securing our country's critical cyber infrastructures. We have a robust higher education system that trains the next generation of cyber security experts, institutions that are developing innovative cyber technologies and one of the nation's most technically advanced workforces. Maryland is among the first states to have already implemented significant cyber security protection initiatives. And, we have a rapidly growing information technology industry cluster that offers the full spectrum of cyber security capabilities.

Our state has tremendous assets to keep the country safe and advance innovations in cyber security. Accordingly, I tasked the Maryland Department of Business and Economic Development to reach out to stakeholders in our state's cyber security community to catalogue these assets and assist in the development of a preliminary response to the President's call to action. I offer my gratitude to all the stakeholders who generously gave their time and energy to this report. This input was invaluable.

One of my most solemn obligations is to safely guard our citizens which includes protection from cyber threats. As Governor of Maryland, Co-Chair of the National Governors Association's Special Committee on Homeland Security and Public Safety and member of the U.S. Homeland Security Advisory Council, I take this responsibility very seriously. I look forward to working with my federal, state, local and private partners to fulfill our responsibility to support this critical national priority and elevate Maryland's leadership in cyber security and information technology.

DEFINING CYBER SECURITY

The National Security Agency defines Cyber Security as "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation."

Cyber security comprises a considerable set of discrete technologies, capabilities and services that stem from and expand on practices of computer information and network security. Information security is now integrated into every computing process in government and business.

Cyber security technology encompasses the software and hardware tools, techniques and processes that protect: information sharing across the Internet; information attacks; information and identity theft; and confidentiality, integrity and availability of data.

Cyber threats are one of the most serious economic and national security challenges we face as a nation. In short, America's prosperity in the 21st century will depend on cyber security.

President Barack Obama

EXECUTIVE SUMMARY

In today's globally interconnected digital and communications information environment, cyber security is necessary to ensure critical support for the U.S. economy, civil infrastructure, public safety and national security. Protecting our nation's information networks requires strong vision and leadership. Under the direction of Governor Martin O'Malley, Maryland is poised to lead in this essential national priority.

Critical sectors of the national economy are now reliant on the effective and secure flow of electronic information and communications systems. Identity theft, network viruses, loss of sensitive information and other malicious activities pose serious threats in the disruption of these crucial information and communication systems.

Recognizing the tremendous importance of information security and Maryland's potential role in defending and protecting our nation's information networks, Governor O'Malley asked the Maryland Department of Business and Economic Development (DBED) to inventory the State's capacity, resources and opportunities in cyber security. DBED convened public and private sector leaders to assess how Maryland could establish a leadership role in this national priority.

KEY FINDINGS >>>>>>>>>>>>>>>>

Overview

The Department of Business and Economic Development (DBED) interviewed 50 Maryland cyber security stakeholders to assess how best to participate in national cyber security activities while simultaneously developing a vibrant industry to create new jobs, drive sustained growth and generate innovations for the benefit of our nation and the state. The interviewed companies are predominantly involved in the federal market, although a significant number also conduct commercial business. DBED reviewed literature and data to benchmark the state's industry cluster and convened relevant agencies to coordinate activities to make Maryland a policy and industry leader. Through the interviews and analysis, DBED identified key assets that could be leveraged as catalysts for short- and long-term growth of the state's cyber security industry.

Market Outlook

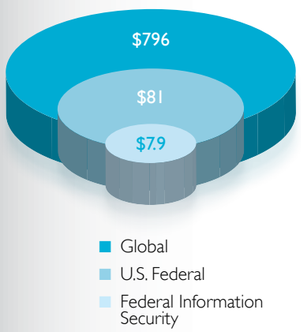
Worldwide information technology (IT) spending is estimated at $796 billion in 2009, with modest growth expected in 2010, according to the Gartner Group. As the top priority of information technology professionals, cyber security represents as much as 20 percent of the average IT budget in most industries. Cyber security is dominated by two distinct but related markets: government and commercial. Although the technologies employed by both are similar, they operate in different spaces because of the level of security issues.

Research from INPUT, a market research firm, estimates the federal IT market alone was $81 billion in 2008, with projected growth to $98 billion in 2013. The demand for information security products and services by the federal government—including civilian, defense and intelligence communities—will increase from $7.9 billion in 2009 to $11.7 billion in 2014.

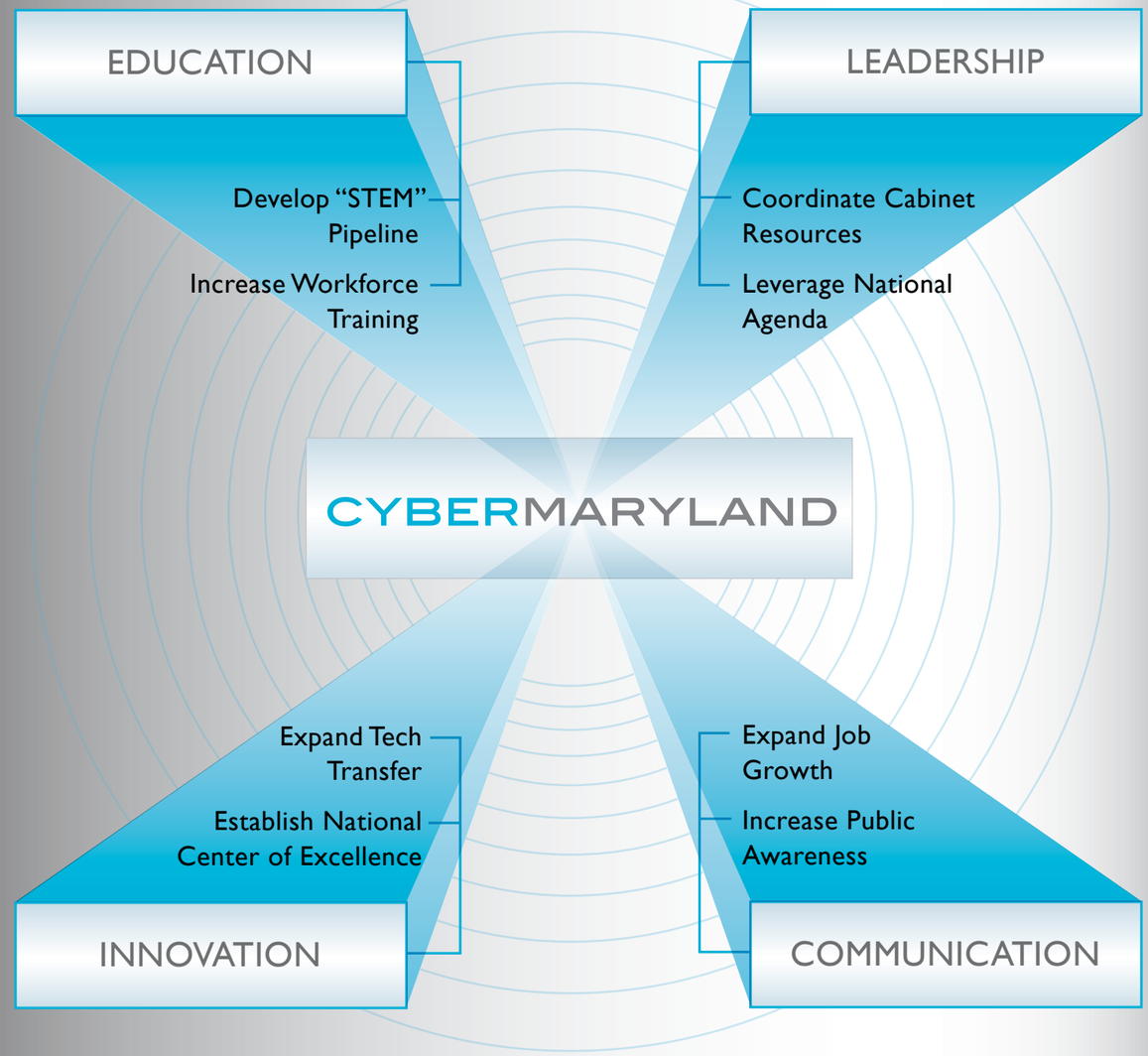
The commercial market for cyber security is estimated to surpass the government market as more entities such as universities, banks and financial service companies and online retailers address the need for information security.

Maryland companies and organizations are optimistic about the continued growth of cyber security efforts; specifically the unprecedented opportunities of Maryland's federal markets, superior workforce, outstanding education system and rich and robust quality of life. Overwhelmingly, stakeholders reported a need for more qualified workers—particularly those who are able to obtain security clearances—as the state's most immediate and significant challenge.

Worldwide Spending on IT Products & Services
(dollars in billions)



CyberMaryland: Epicenter for Information Security & Information



Cyber Crime

According to PandaLabs:

- 50,000 new samples of malware received every day
- Global infection ratio hit all time high in 2009
- Nearly 60 percent of consumers have experienced a computer virus
- U.S. ranks ninth in Global PC Infection Report at 58 percent
- 5 million new strains of malware in three months
- Number of computers infected by malware rose by 600 percent in 2009

The cyber threat is real. Our infrastructure is completely interdependent–power, communications, finance–are all computer-controlled and thus vulnerable.

Kurt Heckman
Sycamore US

Everyone Vulnerable to Cyber Attacks

No industry–from retail to banking to health care to energy–is immune to cyber attacks. As attacks become increasingly sophisticated, computer viruses are a fraction of the problem. Without detection, cyber criminals deliver malicious software to computer networks and then use the **malware** to capture sensitive data or compromise the system. The *CSI Computer Crime and Security Survey* found that dealing with compromised computers is reported to cost an average of nearly $350,000 per organization.

The proliferation of computer-connected electronic devices exacerbates the problem, allowing additional means of entry for criminal activity. **Everything from digital cameras to flash drives to electronic picture frames can carry malware.** Social network sites are targets for cyber thieves who easily breach security to steal user information.

As critical sectors of the nation's economy and service delivery systems become increasingly reliant on the effective and secure flow of information communications systems, protecting data is an economic and national security problem. Growing threats like identity theft and network viruses are part of the ever-evolving world of cyber information security.

Cyber criminals use sophisticated tools to deny service and infiltrate malicious codes in information systems. The next level of threat is state-sponsored cyber attacks or cyber warfare whose targets include critical infrastructure such as electricity grids, transit systems, air traffic control systems, communication networks and banking systems. Disrupting any of these systems can have immeasurable economic impacts.

Secure and safe electronic data transmission is critical to adopt the next generation of new innovations in key economic industries. Information technology can increase efficiency and cost savings in health care and finance. These innovations cannot succeed without a secure system to protect the information. The recent trend toward **cloud computing** also presents new cyber threats and requires new approaches to secure wireless environments.

The path forward requires changes in policy, technology, education and law. **Creating resilient and secure information networks to support the economic growth and national defense in the U.S. must be a priority in Maryland and in the nation.** Opportunities exist for every individual, academia, industry and government to contribute toward this vision.

malware
Malicious code compromising computer data

cloud computing
Information and applications accessible from a shared data center, such as the Internet

The hardest thing we have to do is convince businesses of the need for security because they can't see it. Nine times out of ten, you don't know you're under attack.

Tom Jarboe
Technology Security Associates

A CALL TO ACTION

With the country's intelligence community facing new threats daily, the need to protect the nation's information infrastructure has never been more urgent.

Today's threats are faster, smarter, more prevalent and increasingly elusive. Network breaches are prevalent and cyber crime is a lucrative profession. A recent industry study reported that 50,000 new viruses, worms and other security threats appear every day. The Department of Defense logged 360 million hacking attempts in 2008.

The U.S. is vulnerable due to the widespread interdependence of advanced embedded computer systems in the nation's infrastructure. In business and government, the majority of transactions are created, stored and sent electronically. Business is dependent on information technology and our entire economic system is reliant on computer networks. At the same time, the Internet culture–based on anonymity and free information exchange–greatly enhances the potential for unauthorized use and infiltration.

CYBER SECURITY EPICENTER

As a leader in developing a knowledge-driven economy, Maryland has a critical mass of federal agencies, academic institutions, information technology companies and individuals with the skills needed to secure the nation's infrastructure. Maryland's federal agencies are key leaders in the country's cyber security strategy. Combined with the state's superior security industry cluster, talented human capital and dedicated infrastructure assets, Maryland is poised at the epicenter of national cyber security leadership. Companies are conducting many activities providing and improving information security. In addition to collecting and analyzing data to alert users to threats and improve intelligence, these companies are developing new technologies and using advanced encryption methods to enhance the security of government communications.

Providing Assets for a National Priority

National Investments

President Obama's FY10 Budget request for the Department of Homeland Security included:

- An increase of $75 million for the Department of Homeland Security's Comprehensive National Cyber Security Initiative to develop and deploy cyber security technologies across the world
- Total funding of $37.2 million for research to develop new cyber security technologies
- A $15 million increase for site assistance across the most critical infrastructure and resource sectors to identify vulnerabilities

Maryland's Federal Assets

With NIST, NSA, IARPA and DISA, Maryland is in a position of federal preeminence in cyber security research and development. Their work is complemented by cyber security activities in other major Maryland-based federal agencies and military installations.

National Security Agency (NSA) at Fort Meade conducts basic research in computer, system, data, network and cyber security research and development for national security. NSA is focused on cyber security policy, architecture, research and development, applications development, implementation, technology assessment and testing and standards. NSA funds basic and applied research at colleges and universities in Maryland and across the country, including University of Maryland College Park (UMCP), University of Maryland Baltimore County and Johns Hopkins University.

National Institute of Standards and Technology (NIST) headquartered in Gaithersburg is the oldest federal laboratory and has conducted cyber security research for more than three decades. As the government lead in standards development and protocols for cyber security operations, testing and certification, NIST is involved in basic R&D, application development, implementation and technology. The agency works with the National Science Foundation and the National Academy of Sciences and offers a testing laboratory for cyber products on a fee-for-service basis.

Defense Information Systems Agency (DISA). The technical implementation arm for the Department of Defense (DoD), DISA provides advanced information technology and immediate communications support. As a combat support agency, it plays a vital role in delivering information technology services and capabilities to the war fighter. The agency's mission touches all facets of the DoD information technology environment. DISA is moving from Virginia to Fort Meade in 2011 and will bring approximately 4,300 advanced technology jobs to Maryland.

Intelligence Advanced Research Projects Activity (IARPA). The nation's headquarters for advanced intelligence research, IARPA develops groundbreaking technologies for the intelligence community. Founded in 2007, IARPA is headquartered at UMCP and convenes government, academia and the private sector to improve national security. IARPA consolidated NSA's Disruptive Technology Office, the CIA's Intelligence Technology Innovation Center and the National Geospatial-Intelligence Agency's National Technology Alliance.

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.

U. S. Cyber Command
Planned military command for Armed Services

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.

Military Installations

= 1000 employees

Aberdeen Proving Ground	16
Adelphi Laboratory Center	1
Army Corps of Engineers, Baltimore District	1
Carderock Division, Naval Surface Warfare Center	1
Coast Guard Yard	1
Fort Detrick	5
Fort George G. Meade	36
Joint Base Andrews Naval Air Facility Washington	8
National Naval Medical Center at Bethesda	7
Naval Air Station Patuxent River	9
Naval Support Facility Indian Head	3
Walter Reed Army Medical Center	1

Maryland is the cyber security leader. We house many federal facilities most at risk of cyber attack. We 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

U.S. Naval Academy in Annapolis plans to make cyber security a required field of study for all midshipmen.

Maryland's military installations have an estimated impact of $18 billion on the state's economy. The DoD accounts for half of the procurement spending in Maryland—$12.7 billion in FFY 2008, up 21 percent from the previous year. The U.S. Army ($6 billion) and U.S. Navy ($4.2 billion) are the largest defense contracting agencies in Maryland. All of the top U.S. federal contractors are either based or have a presence in Maryland.

Federal Investments

Non-defense federal procurement purchases of $12.3 billion in 2008 supported more than 200,000 private sector jobs and accounted for more than $17 billion of Maryland's gross domestic product. Maryland is fourth among the states in total federal procurement spending, behind Texas, Virginia and California. Five percent of federal procurement outlays nationwide take place in Maryland. On a per capita basis, Maryland's federal procurement dollars rank third behind the District of Columbia and Virginia.

Maryland has ready access to more than 50 major federal and commercial agencies and research facilities including the Department of Homeland Security, Social Security Administration, the Department of Health and Human Services, the Food and Drug Administration, the Department of Energy, the Nuclear Regulatory Commission, the National Oceanic and Atmospheric Administration, NASA Goddard and the Department of Agriculture Research Center.

R&D: Technology Leadership

Maryland is a hub of research and development activity and home to several of the nation's top research universities including Johns Hopkins University (JHU), the nation's leading university in research volume, as well as the University of Maryland, College Park (UMPC); University of Maryland, Baltimore (UMB); and University of Maryland, Baltimore County (UMBC). Combined, they conduct nearly $1 billion of funded research annually.

Maryland's Blue Ribbon Statistics

- 1st in federal research and development obligations on a per capita basis
- 2nd in the Milken Institute's 2008 State Technology and Science Index
- 2nd in Federal R&D investment ($12.2 billion)
- 2nd in R&D intensity–the ratio of R&D expenditures to gross domestic product by state
- 3rd highest score in the 2008 State New Economy Index (ITIF 2008)
- 7th highest number of computer systems design jobs (57,400) and engineering services jobs (32,000)

What we have in Maryland is access to the agencies who really care about the problem… Maryland companies really have a big advantage in cyber security.

Bill Anderson
Oculis Labs

Maryland's world-renowned academic institutions claim outstanding reputations in computer science research. UMCP, UMBC and JHU are designated by the National Security Agency (NSA) as National Centers of Academic Excellence Research (CAE-R), leading to increased opportunities for grants and contracts with NSA, Department of Homeland Security and other agencies engaged in cyber security work.

The classified world is a unique environment. The sensitive nature of our customers' processes and technologies requires a unique physical environment and a talented cleared workforce. You can't test products out in the open.

Christopher Valentino
Northrop Grumman

CYBER SECURITY RESEARCH LEADERS IN ACADEMIA

Johns Hopkins University	Networking, Wireless, Systems Evaluation, Medical Privacy and Electronic Voting, Emergency Health Preparedness, Bio-terrorism
University of Maryland Baltimore County	Cryptology, Network Security, Intrusion Detection, Quantum Cryptography, Electronic Commerce, Secure Software Agents, Multicast Security, Voting Systems, Health Care Information Systems
University of Maryland College Park	Network Security, Mobile and Sensor Networks, Hybrid Communication Networks, MEMS Sensor Design and Fabrication, Nanotechnology, System Engineering Methodologies, Supply Chain Management, Economics of Information Security
Morgan State University	Bioinformatics

Computer scientist Ross Micheals demonstrates a NIST-developed system for studying facial recognition software programs. The system photographs a person from nine different angles. The photos are analyzed by commercial facial recognition systems. NIST will use research results to support its Congressional mandate to certify biometrics in national entry-exit systems. > > >

Leading Maryland R&D Facilities in IT & Defense

- Johns Hopkins University Applied Physics Laboratory
- Johns Hopkins University Information Security Institute
- UMBC Center for Information Security and Assurance
- Maryland Information Network Dynamics Laboratory
- NIST Information Technology Laboratory
- National Security Agency Research Directorate
- Army Research Laboratory
- Intelligence Advance Research Projects Activity

The US economy has evolved from manufacturing products to manufacturing IT.

Larry Cox
SAIC

Maryland's cyber industry—like the biotech industry—is characterized by small businesses doing very innovative work.

Michael Mourelatos
Proteus

Business Community: Corporate Leadership

Maryland enjoys a substantial advantage in IT jobs, particularly those related to cyber security. This IT industry cluster encompasses establishments that manufacture electronic computing and communications equipment, provide computer systems and other IT services and repair IT equipment. Maryland has the fifth highest concentration in overall IT cluster jobs with a location quotient of 1.6. The ratios are used to compare state employment by industry to that of the nation. A location quotient greater than 1.0 indicates a state industry employment concentration that is greater than the national average.

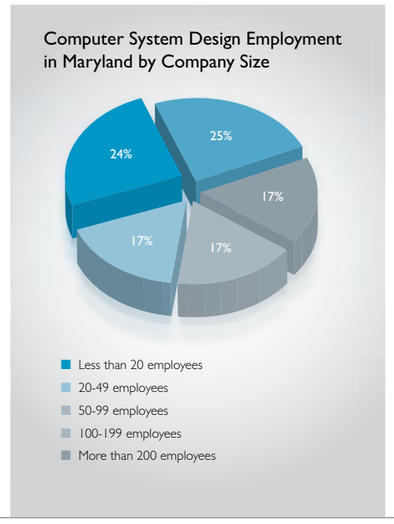
Maryland's Blue Ribbon Stats

- Fifth highest concentration of tech industry workers with 80 out of every 1,000 private sector workers employed by the high-tech industry. (AeA Cyberstates 2008)
- Second in the nation in professional and technical workers as a percentage of the workforce, with more than 220,000 workers employed in professional, scientific and technical service industries
- First in employed doctoral scientists and engineers per 100,000 employed workers
- Seventh in computer and information sciences doctoral scientists

Maryland IT employment is dominated by firms that provide computer systems design, a linchpin of cyber security activities. With more than 60,000 jobs, this subsector comprises nearly seven out of every 10 IT jobs in Maryland, the seventh highest in the country. These firms are engaged in IT technical consulting, application provisioning, business process management, data storage, data management and custom computer application design and development. Maryland has a particularly significant advantage in computer systems design employment with a 2.2 location quotient, third highest in the country. Maryland has the country's second highest concentration in custom computer programming services employment with a 2.0 location quotient, and the third highest in computer systems design services with a 2.6 location quotient.

Profile

Oculis Labs in Hunt Valley develops technology solutions to protect the 'last two feet' in cyber security: the distance between the computer screen and user. Chameleon, a high security product for classified government use, employs a special camera that calibrates to the user's eyes allowing only that person to view the data clearly. PrivateEye is the companion retail product. Oculis is also an affiliate member of Howard County's NeoTech Incubator.



Computer systems design is dominated by smaller businesses, particularly in Maryland. The state has more than 5,500 computer systems design firms with fewer than 20 employees. These firms employ almost 15,000, an average of 2.7 employees per company. The average size of a computer systems design establishment in Maryland is 10 employees. Nearly six out of 10 computer systems design employees in Maryland work in businesses with fewer than 100 employees.

Profile

Sourcefire was founded in 2001 by Martin Roesch, author of Snort®, the world's most popular intrusion detection and prevention technology. The Columbia-company grew from a venture-backed startup that went public in 2007. Maryland was an early investor through the Challenge Investment program. Sourcefire's real-time technologies are used by every military branch and half the Fortune 500 companies. Their federal business almost tripled from 2007 to 2008.

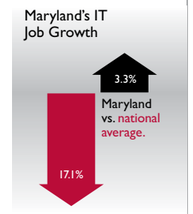
Top Maryland Defense IT Contractors
Boeing
Booz Allen Hamilton.
CACI International
Computer Sciences Corporation
General Dynamics Corporation
Honeywell International
IBM
L3 Communications
Lockheed Martin Corporation
MITRE
Northrop Grumman Corporation
SAIC

Some of these smaller companies are borne out of university and government research and represent opportunities for innovation and growth. Many cyber security companies have been formed by former government, military and intelligence workers.

Maryland also has many of the large systems integrators that are doing work in cyber security. Systems integrators build IT solutions. They specialize in integrating technology, strategy, policy and operations. They provide opportunities for small businesses by sub-contracting portions of large government contracts.

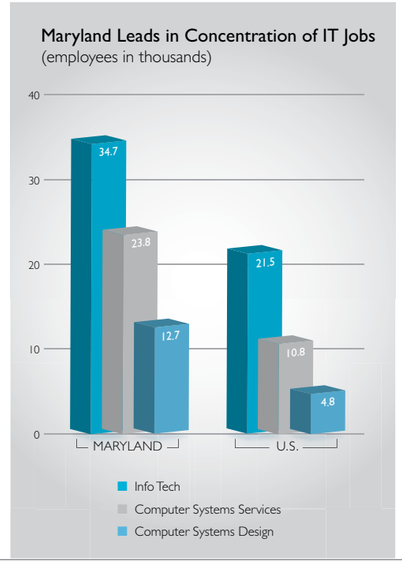
Maryland also has many of the large systems integrators that are doing work in cyber security. Systems integrators build IT solutions. They specialize in integrating technology, strategy, policy and operations. They provide opportunities for small businesses by sub-contracting portions of large government contracts.

Over the last decade, Maryland's IT advantage has increased substantially. **During 2001-2008, while nationwide IT employment fell by 17.1 percent, Maryland IT employment rose by 3.3 percent. Among the states with high IT concentrations, Maryland is one of the few that added jobs in 2009.** From November 2008 to November 2009 Maryland had the nation's top ranked growth rate (7.2%) in computer services employment.



All the players in the cyber community are either headquartered here or doing work here.

Theresa Harrison
Premier Management Corporation

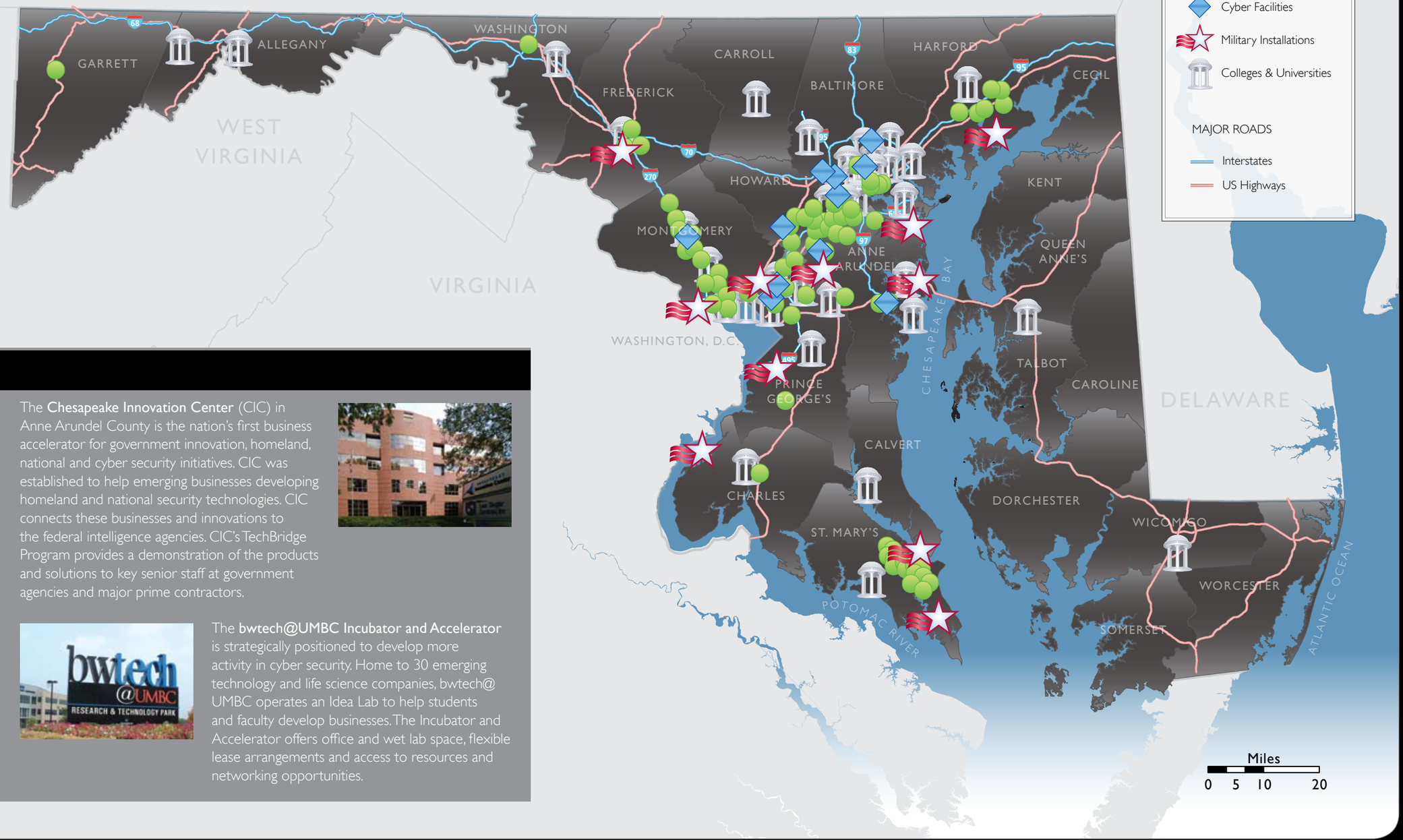


Maryland has one of the highest concentrations of technology jobs in the country, with approximately 10 percent of jobs classified as technology related. Approximately half of those jobs are related to information technology, telecommunications and engineering. Maryland has an estimated 9,500 private sector technology businesses, employing more than 126,000 people.

Maryland: The Epicenter of Cyber Security

Maryland's location is strategic for defense contractors, IT companies and researchers in cyber security.

Fifty federal agencies and research facilities are located in Central Maryland. Three international airports provide global market access. A separate power grid from New York makes Maryland an ideal location for secure back-office operations. The State has a fiber-rich, redundant and reliable telecommunication network valued at $5.5 billion to support cyber security activities.



Growing Cyber Presence

Millions of square feet of new development are centered around Naval Air Station Patuxent River, Aberdeen Proving Ground and Fort Meade. National Business Park, a 285-acre business community in Anne Arundel County houses government contractors and expects to gain additional tenants from federal cyber security initiatives. Developments include Sensitive Compartmented Information Facility space and secure facilities. Across the state, more than 20 business incubators offer shared resources, access to state-of-the-art equipment and facilities and business assistance.

The **Chesapeake Innovation Center** (CIC) in Anne Arundel County is the nation's first business accelerator for government innovation, homeland, national and cyber security initiatives. CIC was established to help emerging businesses developing homeland and national security technologies. CIC connects these businesses and innovations to the federal intelligence agencies. CIC's TechBridge Program provides a demonstration of the products and solutions to key senior staff at government agencies and major prime contractors.

The **bwtech@UMBC Incubator and Accelerator** is strategically positioned to develop more activity in cyber security. Home to 30 emerging technology and life science companies, bwtech@UMBC operates an Idea Lab to help students and faculty develop businesses. The Incubator and Accelerator offers office and wet lab space, flexible lease arrangements and access to resources and networking opportunities.

Education: Academic Leadership

Maryland's schools are among the nation's best at preparing students for advanced study and careers. *Education Week* ranked the State's public school system first in the nation in its *Quality Counts Report* on high school graduation, student achievement, academic standards and accountability. One-third of Maryland's 2008 high school graduates completed the minimal math and science coursework that will allow them to enroll in college level science, technology, engineering and mathematics (STEM) courses.

To meet Maryland's growing demand for a workforce trained to fill jobs in information security and the knowledge-based economy, the state is developing an education pipeline to produce highly skilled workers trained in Science, Technology, Engineering and Mathematics disciplines. Recognizing the importance of STEM education and research for Maryland's future well-being, Governor O'Malley established the STEM Task Force of the P-20 Leadership Council of Maryland. The Task Force developed future-oriented priority recommendations to ensure Maryland's ability to prepare its students to meet the demands of a growing STEM-based economy. The August 2009 STEM Task Force Report will strengthen STEM programs at all levels of education in Maryland.

We have the best cyber security talent in the world in Maryland.

Larry Fiorino
G1440

There exists today a shortage in supply of talented employees both entering the workforce and also those developing into senior leaders.

Christopher Valentino
Northrop Grumman

Cultivating a high quality workforce starts at grade school level. The state's focused attention on STEM disciplines will positively impact both the K-12 classrooms and the growing STEM-based private sector. There are currently successful K-12 programs in Maryland that develop human capital assets:

- **Anne Arundel County Public Schools** offers suites of STEM academic and co-curricular offerings for pre-K-12 students during the academic year and summer to enrich learning, build career awareness and engage students in challenging projects and events. Anne Arundel County Public Schools, with 74,000 students, is launching its signature **homeland security program** in fall 2010 with 100 to 200 freshmen at Meade High School. The program includes specially designated English, science and history classes with an emphasis on Homeland Security, utilizing real-world curricula and activities.
- **Harford County Public Schools,** with 40,000 students, kicked off the nation's first **homeland security school program** this year with 60 sophomores at Joppatowne High School. The program will expand to 180 students (grades 10-12) in coming years.
- **Baltimore County Public Schools,** in collaboration with Johns Hopkins University Center for Technology in Education and software engineers at the Johns Hopkins University Applied Physics Laboratory (JHU/APL) have developed a prototype **Virtual Learning Environment** at Chesapeake High School to provide a game-like experience to augment existing math and science curricula. The first of its kind in the nation, the VLE is housed in a new facility modeled after APL's state-of-the-art, 3-D visualization facility used for DoD and NASA projects.

< < < Governor Martin O'Malley and Lt. Governor Brown celebrate Maryland's top public school ranking.

Workforce: Advanced Education Leadership

Maryland offers the most exciting job market for cyber in the country.

Rosemary Budd
Booz Allen Hamilton

We have made a conscious decision to work with government and private sector of where we are located. There is a tremendous opportunity for young people to work with cyber companies for DISA.

Dr. Eugene DeLoatch
Morgan State University
School of Engineering

Students come to UMBC because of the options to work for the federal government, defense contractors, and in other technical fields.

Dr. Charles Nicholas
UMBC Department of Computer Science and Electrical Engineering

With the increased demand for workers trained in specialized information technology disciplines, institutions of higher education across the country are developing programs to train graduates in information security. As a result of National Security Agency (NSA) and other government agencies' proximity, Maryland's institutions of higher education have developed expertise in cyber security.

More than 20 colleges and universities in Maryland currently offer degrees in computer science and many also offer internships and cooperative training in computer science. **Six state universities are certified by the NSA as Centers of Academic Excellence** (CAEs). These schools serve as regional centers of information assurance expertise and provide programs to retool and retrain federal and state IT personnel. Students attending these designated schools are eligible to apply for scholarships and grants through the **Department of Defense Information Assurance Scholarship Program.**

Johns Hopkins University offers the **Federal Cyber Service Scholarship for Service,** a unique program funded by the National Science Foundation to increase and strengthen the number of federal information assurance professionals. The scholarship fully funds all education costs (books, tuition and room/board). Students also receive stipends of up to $8,000 for undergraduate and $12,000 for graduate studies.

The University of Maryland College Park (UMCP) was recently ranked among the top ten universities in preparing future cyber security professionals, according to The New New Internet, a web site devoted to cyber security. UMCP produces the largest number of STEM graduates in the state and is the only public university on the East Coast with top 20 programs in math, physics, computer science and engineering. The Institute for Advanced Computer Studies operates more than 17 laboratories with many devoted to security research.

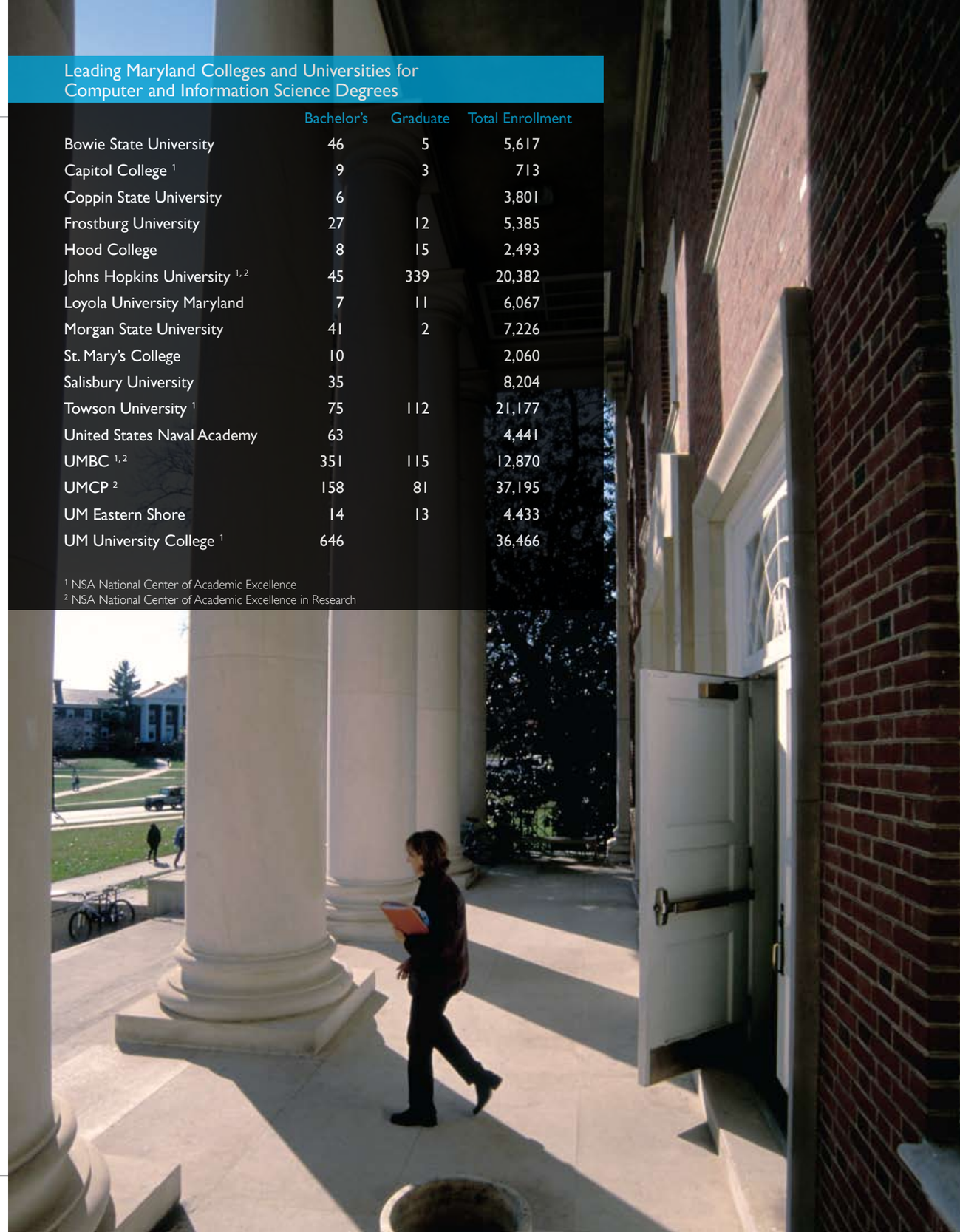
The University of Maryland, Baltimore County (UMBC) has the second highest percentage of students in STEM fields of any university in the country, behind only the United States Naval Academy in Annapolis. UMBC's **Center for Information Security and Assurance** (CISA) promotes research, education and sound internal practices in information security and assurance. **UMBC Training Centers** deliver non-credit information security training programs for industry and professional certifications in Information and Network Security, Core Industry and DoD 8570 Certification Courses, Network Security and Administration, Secure Software Development, Computer Forensics and Penetration Testing.

Maryland's 16 community colleges operate a network of 23 campuses and many learning centers throughout the state. Anne Arundel Community College (AACC) was the first community college in the country to develop a cyber security curriculum and the first certified by NSA to map its courses to the 4011 training standard for information security professionals in federal government. AACC's **Information Systems Security** program offers an Associate of Applied Science degree, certificate and courses to prepare students for entry-level positions in cyber security. Students in the program are prepared to sit for several industry certifications and many transfer to four-year institutions with third-year status. AACC is an active member of the CyberWATCH center, a National Science Foundation funded consortium dedicated to increasing the cyber workforce.

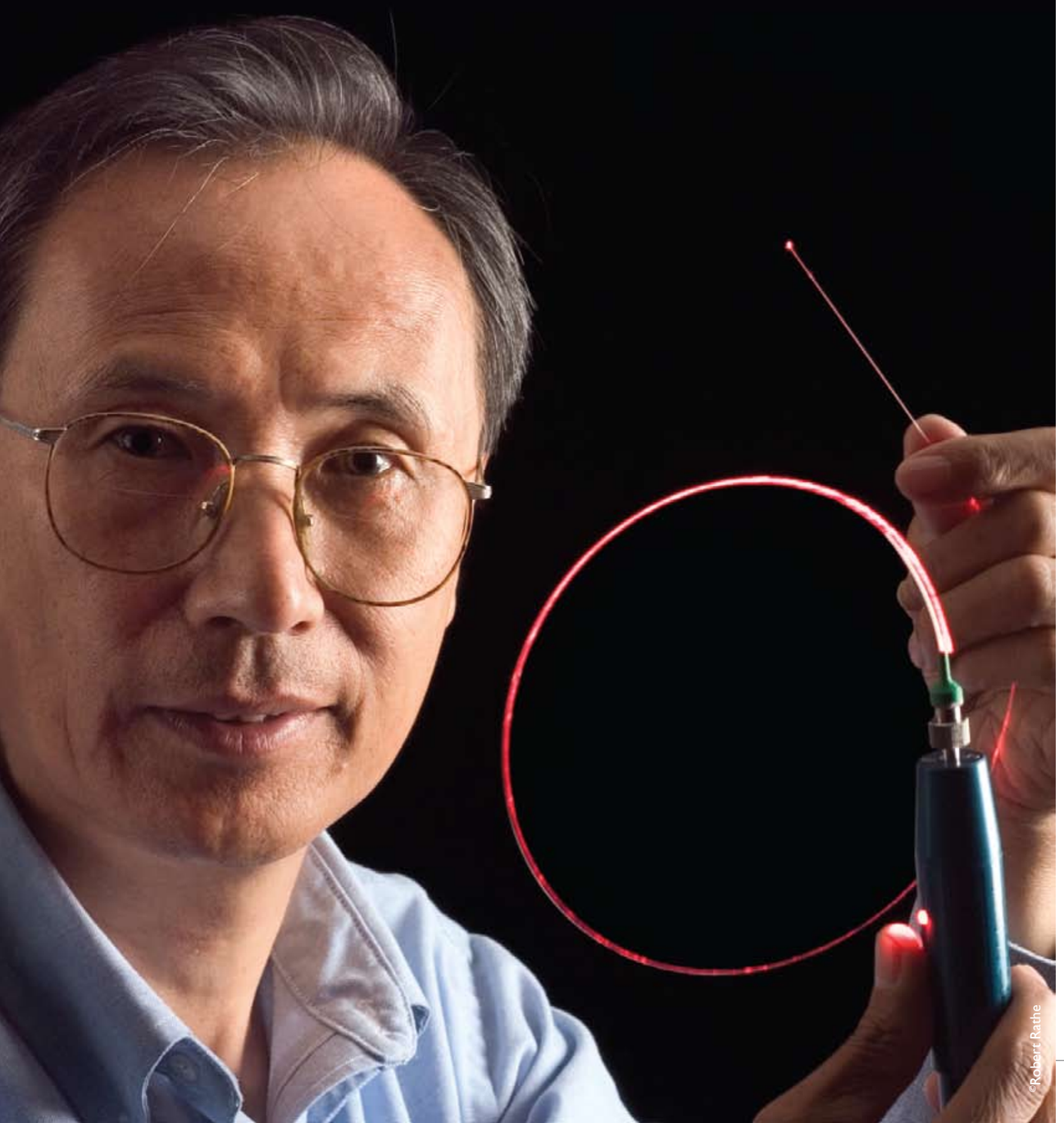
Leading Maryland Colleges and Universities for Computer and Information Science Degrees

	Bachelor's	Graduate	Total Enrollment
Bowie State University	46	5	5,617
Capitol College [1]	9	3	713
Coppin State University	6		3,801
Frostburg University	27	12	5,385
Hood College	8	15	2,493
Johns Hopkins University [1, 2]	45	339	20,382
Loyola University Maryland	7	11	6,067
Morgan State University	41	2	7,226
St. Mary's College	10		2,060
Salisbury University	35		8,204
Towson University [1]	75	112	21,177
United States Naval Academy	63		4,441
UMBC [1, 2]	351	115	12,870
UMCP [2]	158	81	37,195
UM Eastern Shore	14	13	4.433
UM University College [1]	646		36,466

[1] NSA National Center of Academic Excellence
[2] NSA National Center of Academic Excellence in Research



Quantum Communications Over Optical Fiber Channels – NIST physicist Xiao Tang and colleagues have developed a quantum communications system that uses single photons to produce a "raw" encryption key at the rate of 4 million bits per second.



©Robert Rathe

The Path Forward to Strengthen Maryland's Cyber Security Leadership

PRIORITY ONE

SUPPORT THE CREATION AND GROWTH OF INNOVATIVE CYBER SECURITY TECHNOLOGIES IN MARYLAND

Cyber security and information innovation technologies represent an unparalleled economic and employment growth opportunity for Maryland.

Allen Shay
Prescint

Adding security as an afterthought does not work. It is possible to make computer systems more secure than in the past but we are dealing with legacy systems and trying to make them secure.

Dr. Charles Nicholas
UMBC Department of Computer Science and Electrical Engineering

1. Establish a National Center of Excellence for Cyber Security

Given the vast cyber security assets in the state, Maryland is an ideal location for a federally-recognized National Center of Excellence for Cyber Security. Working closely with the Maryland congressional delegation, state leaders can identify initial federal funding for a pilot program for the Center of Excellence for Cyber Security and seek official statutory designation for the Center of Excellence.

A model for establishing this center would be a partnership involving government, private corporations and academic institutions that incorporates the following elements:

- **Incubator.** Determine the feasibility of establishing an incubator for firms developing cyber security products and new technologies focused on national security, including the possibility of establishing a virtual incubator or co-locating at an existing location.
- **Cyber Security Testing Laboratories.** Focus on testing hardware and software products for operational readiness and meeting cyber security standards, and certifying and validating through testing that these IT products operate at their stated security levels.
- **Cyber Security Auditing Capability.** Conduct an annual IT security audit of each government agency funded with State dollars to help ensure the security, confidentiality and integrity of all state data network and control systems; these services can also be provided on a fee-for-service basis to other entities.
- **Information Sharing.** Create a clearinghouse for sharing information about vulnerabilities and risks identified in commercially available hardware, software and IT systems.
- **Education and Training.** Develop cyber security training packets for schools. Integrate IT and data security issues with technology education at every level throughout the education system.
- **Cyber Security/IT Law Council.** Advise the Governor and state leadership

on cyber security and IT policy issues, assist the Governor in conjunction with the state legislature and develop tactical actionable enforceable state laws and regulations that protect citizens and businesses.

Maryland must partner with the federal government to ensure that adequate law, policies and resources are available to support the cyber security mission. The state should work with the federal government to recommend and implement coherent unified policy guidance where necessary. State government has an important role to play in this area, by enacting state laws and regulations that can fill gaps left by federal laws and regulations and address the needs of Maryland citizens. For example, Maryland recently enacted laws to protect its citizens from identity theft.

Cyber is more than information security… to conduct security you have to understand a hacker. We need tools such as predictive modeling to find out who is attacking and understand what is going on from a behavior perspective.

Michael Mourelatos
Proteus

Potential policies that must be reviewed include privacy and governance issues. In an age of social networking and broad use of the Internet–not only to conduct business, but also to communicate with friends and family–it is much more difficult to control the information that is revealed about a person, as well as access to that information. Privacy measures to protect personal information are now provided in some social networking sites. In the final analysis, however, it is the user's responsibility to choose what information is provided and what security settings are applied. With the advent of cloud computing, the issue of privacy moved to the forefront. Cloud computing raises new concerns, such as who is storing the data in "the clouds" or cyberspace, who has access to the data and how does one know if the data has been compromised and an individual's privacy has been violated. The conflict between the need to share information and the need to protect that information is the subject of policy research and debate.

2. Encourage Cyber Security Technology Transfer & Commercialization

The Federal government and defense is where cyber security technology gets started before it moves to the marketplace.

Rodney A. Pieper
EDS/HP

Cyber security technologies transferred from the federal laboratories and universities in the state can become an engine for Maryland-based economic development and growth. This technology transfer will create opportunities for entrepreneurship and innovation. Although Maryland is ranked high in R&D spending, greater attention should be focused on improving technology transfer and commercialization of R&D products and services.

Maryland's business community is excellent. The network of contacts I've made is fantastic and far surpassed anything (I had) in Silicon Valley.

Bill Anderson
Oculis Labs

Maryland can work with the federal government and industry to effectively and efficiently transfer cyber security research results into commercial products and to build an innovative cyber security workforce. The Maryland Technology Development Corporation (TEDCO) should employ its statutory authority to enhance its leadership role in the cyber security technology transfer in the State. TEDCO should also seek creative new approaches to technology transfer that will maximize commercialization so that Maryland-based technologies can more readily enter the marketplace. In this manner, TEDCO can help push for the realization of the potential benefits of this research.

A catalogue of cyber security work being performed throughout Maryland can be developed in order to establish a baseline, measure progress and obtain an accurate assessment of the state's demographics. This catalogue can also be used as a tool to share research and foster collaboration opportunities. The state should emphasize programs that will translate mature or near mature R&D to the commercial marketplace through a robust program for entrepreneurship.

Defense agencies perform highly sophisticated work and there are a relatively few people doing that work. Maryland is poised to increase commercial opportunities as more businesses respond to the need for web security.

Larry Fiorino
G1440

SafeNet has succeeded by being entrepreneurial… we invested our own money in R&D and leveraged our commercial roots to sell to the government.

Joe Moorcones
SafeNet

Co Profile

Smartronix specializes in NetOps, cyber security, eEnterprise software solutions, mission focused engineering and health IT. Headquartered in Hollywood, Smartronix has locations around the world and has been recognized as one of the nation's fastest-growing companies. They provide customized portable security systems for mobile and wireless data communications and products to protect laptop interfaces, power converters and wireless adapters.

Given the value and the challenges of technology transfer, there should be support to transform existing and future cyber security research results into commercial products or operational best practices. These measures could include efforts to strengthen the development of metrics, models, datasets and testbeds so that new products and best practices can be evaluated, as well as the development of a database of results from cyber security research that allows vendors to identify ideas that can be incorporated into commercial products.

3. Enhance Maryland's Information Standards, Certification & Testing Capabilities

Maryland has an opportunity to grow the cyber security industry cluster by encouraging either the creation of new businesses or expanding the capabilities of existing business in cyber security standards, certification, testing, auditing and assessment.

Cyber security standards comprise a set of policies and guidelines that allow organizations to practice safe security techniques to minimize the number of cyber attacks. ISO/IEC 27002 is the most commonly used. Certification allows the organizational entity to be recognized as compliant with the standards. A certification authority should be established.

Testing laboratories evaluate cyber security tools and techniques–including hardware, software, network and communication tools and devices–for capabilities, usability and conformance. The National Security Agency (NSA) and and National Institute of Standards and Technology (NIST) operate assessment laboratories and NSA issues a certified product list. Although both organizations have assessment laboratories, the capacity of these laboratories may be strained with the potential explosion of tools in the marketplace to address the increasingly vulnerable internet. The state could play a part in performing technology assessments for cyber security tools.

In order to carve out Maryland industry opportunities in cyber security certification, standards and testing, it may be necessary to conduct a feasibility analysis for establishing a test laboratory and certification businesses for cyber products in the state.

Measures should be taken to grow Maryland's cyber security businesses and to create new jobs by working with the Governor's Grants Office and by collaborating with federal cyber security programs and tapping into appropriated funding to secure federal agency networks. These measures will increase the procurement opportunities for Maryland companies in obtaining federal cyber security funding.

PRIORITY TWO

DEVELOP AN EDUCATIONAL PIPELINE TO TRAIN NEW CYBER SECURITY TALENT AND ADVANCE WORKFORCE DEVELOPMENT

The process for gaining security clearances has improved recently, but it is still a long process.

Elizabeth Rendon Sherman
LinguaIISTek

Because there is a shortage of people with the right skills, the key is developing those people.

Sarah Djamshidi
Chesapeake Innovation Center

4. Align Maryland's Education Programs to Meet Demand for Cyber Security Talent

Industry and government will continue to need more workers in cyber security. Maryland must be poised to provide the talent to meet future needs. However, the state is experiencing a shortage of highly qualified STEM (science, math, engineering, and mathematics) workers. Maryland has approximately 6,000 STEM openings a year and produces approximately 4,000 STEM graduates. A 2007 National Academies report, *Rising Above the Gathering Storm*, indicated that the U.S. is in a perilous position as colleges and universities in the U.S. and across the world are minting new foreign-born scientists, mathematicians and engineers at a rapid pace. Of the 30 fastest-growing occupations projected through 2016, the U.S. Bureau of Labor Statistics' *Occupational Outlook Handbook* concludes that 16 require substantial mathematics or science preparation.

Despite the numbers of graduates coming out of universities in the state, more must be done to encourage students to consider cyber security careers and prepare for work in the field. There are two issues: universities need to attract American-born students into IT programs, and students must be aware obtaining a security clearance requires smart and safe lifestyle decisions.

Measures may include:

- **Focus academic efforts on STEM** and cyber security disciplines outlined in the *Final Report of the Governor's STEM Task Force*. The Task Force—part of the P-20 Leadership Council of Maryland—presented Governor O'Malley with recommendations to prepare students for a growing STEM-based economy, including tripling the number of teachers and increasing the number of STEM college graduates 40 percent by 2015.
- **Develop scholarships** or other honors to encourage high school graduates to remain in Maryland for college. According to the Southern Technology Council, 70 to 75 percent of the students who leave their home state (including Maryland) to attend college do not return.

< < < The Johns Hopkins University Applied Physics Laboratory's National Information Assurance Engagement Center (NIAEC) is developing mechanisms to correlate cyber warfare with kinetic missions.

There is a huge range of skill levels and job opportunities in information assurance—from technical and design of counter measures, to diagnostics and forensics.

Dr. Charles Nicholas
UMBC Department of Computer Science and Electrical Engineering

Students need to come out of school with certification and clearance already in hand.

Lee Holcomb
Lockheed Martin

After the dotcom bust, students stopped going into IT. Now they recognize the merit but there have to be incentives for students to persue government agencies and contractors.

Gerald Masson
Johns Hopkins Information Security Institute

- **Provide incentives** for college graduates to remain in the state. Although Maryland is the home of the premier government agencies, competition for talented graduates is intense.
- **Review the curriculum** at two-year colleges or community colleges to develop a certificate program for cyber security, to create a pipeline of younger workers with the skills to fill the technician jobs in cyber security, and to address some of the growing issues in cyber security.
- **Train teachers** in cyber security. Address the shortage of qualified teachers at all levels by providing targeted training and offering incentives to stay in Maryland.

5. Develop Workforce Training Programs to Address Industry Needs

As cyber security industries grow, there is a growing demand for skilled workers eligible for security clearance and a severe shortage of qualified workers to fill these jobs. The gap is fueled by the strong federal technical and research presence and the high number of federal workers retiring or expected to retire in the near future.

Meeting workforce demands will become more challenging when the Defense Information Systems Agency begins its move to Fort Meade in 2010. Moreover, with President Obama's recent initiative to "in-source" organic functions in federal agencies, as opposed to contaracting out those fundtions, demand for skilled workers in federal government will increase. Some functions in the cyber security area fall under this mandate. These factors all contribute to anticipated workforce pressures as both government and industry seek trained and talented workers.

Cyber security requires a workforce that is ready to meet the field's technical and policy demands. Meeting the future workforce needs requires that we address formalized educational institutions and complement those measures with other workforce training initiatives such as:

- Develop an academic cyber security curriculum for degree or certification at the post-secondary level, community colleges, four-year colleges and universities.
- Develop a skills gap analysis to identify specific training needs in cyber security work.
- Retrain workers with obsolete skills in areas that are in high demand, including all disciplines of cyber security.
- Create a public-private partnership jobs network for recruitment and training.
- Establish a relationship with the Department of Defense's Cyber Corps Program, a federal program that trains students in systems security and related engineering and science disciplines, and retain graduates in Maryland.

PRIORITY THREE

ADVANCE CYBER SECURITY POLICIES TO POSITION MARYLAND FOR ENHANCED NATIONAL LEADERSHIP

Information security must be tightly woven into the fabric of all information solutions.

Lee Holcomb
Lockheed Martin

6. Coordinate a Cabinet-level Review of Cyber Security Actions

Governor O'Malley directed the State to support the President's efforts to make core digital infrastructure a priority. The National Governors Association identified cyber security as a state's weakest link in protecting its critical infrastructure.

Agencies such as Maryland's Departments of Business and Economic Development (DBED), Information Technology (DoIT), Labor Licensing and Regulation (DLLR) and the Maryland Higher Education Commission (MHEC) are coordinating activities to make the state a policy and industry leader in cyber security. These agencies are engaged in a multi-faceted, public-private approach involving the breadth of Maryland's cyber security strengths to better protect computer systems and personal information from attack.

Preliminary activities include:

DBED Developed a benchmark analysis of the state's cyber security industry cluster. Reviewed federal policy, technology developments and industry trends. Assessed education programs, workforce needs and federal procurement. Created the Federal Facilities Advisory Board to formulate and execute policy recommendations.

DLLR Developed a workforce assessment and survey. Cyber security workforce efforts expected to complement workforce initiatives related to DoD activities.

DoIT Established Maryland as a national leader in securing public electronic infrastructure and private information. Established a *Cyber Security Policy* based on accepted best practices and provided cyber security awareness training to state agencies and assisted public and private organizations.

MHEC Determined university and community college curriculum and capacity needs for developing the cyber security workforce.

The May 2009 White House Cyberspace Policy Review expressed the need to elevate cyber security as an issue among every state by designating a single state leader to ensure effective coordination between Chief Information Officers, chief information security officers and state homeland security advisors. Governor O'Malley actively supports the President's recommendation and intends to appoint an individual to direct and coordinate the technical aspects of cyber security throughout the State information systems.

7. Align Maryland State Cyber Security Priorities with those of the President's Cyber Security Priorities

Everybody has a part in the cyber mission. We will have some catastrophic consequences if we don't act.

Michael Mourelatos
Proteus

To address threats to the U.S. information and communications infrastructure, the President has outlined action plans for the federal government to build capacity for a digital nation, share responsibility for cyber security, create effective information sharing and incident response systems and encourage cyber security innovation. As the state experiences many of the same network intrusions and infections as the federal government, and is home to a large number of critical federal cyber security facilities, Maryland should seamlessly align its priorities to match those of the federal government.

To prevent, detect and respond effectively to cyber security breaches, information must be shared across all levels. State and federal governments must work together and in conjunction with the private sector to share information that helps detect sophisticated intrusions or attacks. A full understanding and the most effective cyber security response may only be possible by bringing information from all sources together.

The culture of the Internet is anonymity and freedom. Privacy issues make it difficult to determine who is originating cyber attacks.

Lee Holcomb
Lockheed Martin

The State should work with the federal and local governments to develop options for cyber security information sharing that address concerns with homeland security, as well as privacy and proprietary information. The Governor, through the agencies, should develop an effective structure to administer, manage and develop strategies to ensure the security and resilience of infrastructure systems and information sharing. This structure should also address state homeland security and the continuity of operations for the public and private sector.

8. Create a Multi-Faceted Communications & Marketing Strategy to Increase Public Awareness

While government is responsible for ensuring the safety and well-being of citizens, the private sector designs, builds, owns and operates most of the network infrastructures that support government and private users alike. Industry and governments share responsibility for a secure and reliable infrastructure.

Broad public awareness of the risks of online activities and strategies Maryland can adopt to reduce those risks requires an effective communications strategy. The State can partner with federal and local governments, educators, industry, the civil liberties and the privacy communities to conduct a Maryland cyber security public awareness and education campaign. The public education and awareness campaign must increase awareness of the threat and make recommendations on enhancing digital safety and security.

Other states can claim cyber, but we have the core of expertise.

Michael Mead
CACI

We started out as an 8A (small contractor) and partnered with the big defense contractors. Now we've graduated from the program and are positioning ourselves as a prime contractor.

Elizabeth Rendon Sherman
LinguaIISTek

The commercial side of cyber security will be as big as that of the government if not bigger. Cyber Security is global.

Larry Cox
SAIC

PRIORITY FOUR

ENSURE THE SUSTAINED GROWTH AND FUTURE COMPETITIVENESS OF MARYLAND'S CYBER SECURITY INDUSTRY

9. Market Maryland as the National Epicenter for Cyber Security

With the vast and incomparable assets in the state, Maryland is already a national epicenter of federal cyber security efforts. Maryland's cyber security brand must be strengthened and advanced to foster proactive outreach and marketing to targeted information technology industry segments, both domestically and internationally.

The Maryland Department of Business & Economic Development should take the lead to develop and implement a coordinated and defined marketing campaign in conjunction with economic development organizations including the Technology Council of Maryland, the Maryland Economic Development Association and county economic development offices. This campaign would raise Maryland's visibility in the cyber security industry both nationally and globally by generating and qualifying attraction prospects, engaging Maryland cyber security leaders as partners and helping to attract qualified prospects. The campaign will highlight Maryland's cyber security assets and opportunities.

10. Identify Future Growth Opportunities & Implement an Economic Development Strategy for Cyber Security

Maryland can build on its assets and position as a cyber security leader by developing and expanding further business opportunities. International and domestic companies seek to locate in Maryland to take advantage of access to federal agencies. Existing Maryland companies, particularly small businesses, can capitalize on the potential for contracting and research partnerships. New companies can emerge around promising new technologies and needed capabilities such as testing and certification.

The Maryland Federal Facilities Advisory Board (FFAB) has been created in cooperation and support for ongoing Maryland cyber security initiatives.

ACKNOWLEDGMENTS

A project of the State of Maryland, Department of Business & Economic Development

Many individuals provided information and input for this important effort. I offer my sincere appreciation to the many industry experts who participated in this initiative. I also want to acknowledge the Department's staff and state partners who helped compile, review and develop the recommendations.

Christian S. Johansson, Secretary

Andréa Vernot, Assistant Secretary, Marketing and Communications

Ben Wu, Project Director

Nancy McCrea, Research Director

Veronica Dorry, Creative Director

Maureen Kilcullen, Editor

Bill Anderson, CEO
Oculis Labs Inc., Hunt Valley

Rosemary Budd, Principal
Booz Allen Hamilton, Annapolis Junction

John Burris, CEO
Sourcefire, Columbia

Larry Cox, Senior V.P. & G.M.
SAIC Intelligence & Info. Solutions, Columbia

Tom Davis, Chief Technology Officer
Technology Security Associates, Inc.
Lexington Park

Eugene M. DeLoatch, Ph.D., Dean
Morgan State University, Baltimore

Sarah Djamshidi, Executive Director
Chesapeake Innovation Center, Annapolis

Larry Fiorino, President and Founder
G1440, Baltimore

Tim Galpin, Infocentric Operations
Business Area Executive
Johns Hopkins University Applied Physics Lab, Laurel

Patrick Gorman, Strategic Cyber Head
Booz Allen Hamilton, McLean, VA

Andre Gudger, Founder
Solvern Innovations, Baltimore

Theresa Harrison, Senior Vice President
Premier Management Corporation, Baltimore

Kurt Heckman, President & CEO
Sycamore.US, Frederick

Ellen Hemmerly, Executive Director
bwtech@UMBC, Baltimore

Harold Herndon, Sr., President & CEO
Compliance Corporation, Lexington Park

Deborah K. Higgins, Academic
Program Manager
Johns Hopkins University, Baltimore

Lee B. Holcomb, V.P., Strategic Initiatives
Lockheed Martin, Gaithersburg

Tom Jarboe, Chief Operating Officer
Technology Security Associates, California

Arshed Javaid, President & CEO
Smartronix, Hollywood

Mark Kestler, Program Manager
CACI, Lexington Park

Jon Lau, Program Manager,
UMBC Training Centers, Baltimore

Belkis Leong-Hong, President
Knowledge Advantage, Inc., Gaithersburg

Michael P "Rick" Lipscomb, Site Director
The Boeing Company, Annapolis Junction

David MacRae, EVP
Smartronix, Hollywood

Gerald M. Masson, Ph.D., Director
Johns Hopkins University, Baltimore

Marcus McInnis, Director of CCSI Operations
Lockheed Martin, Gaithersburg

Michael Mead, VP Special Programs Division
CACI Systems, Lexington Park

Joe Moorcones, V.P. & G.M.
SafeNet Inc., Belcamp

Mike Mourelatos, Vice President
Proteus Technologies, Annapolis Junction

Charles K. Nicholas, Ph.D., Chair
UMBC CISA, Baltimore

Glenn Nick, Director
Delex Systems, California

Michele Perry, Chief Marketing Officer
Sourcefire, Columbia

Dhananjay S. Phatak, Associate Professor
UMBC, Baltimore

Robert Phibbons, Vice President
iNovex, Annapolis

Rodney A. Pieper, Director, Network Security
EDS, Herndon, VA

John T. Pinkston, Ph.D., Professor
UMBC, Baltimore

Elizabeth Rendón-Sherman, President & CEO
LinguaLISTek, Columbia

Marnie S. Salisbury, Executive Director
MITRE, Annapolis Junction

Allen Shay, President
Prescint LLC, Baltimore

Greg Simmons, Vice President
UMBC, Baltimore

Bob Smout, Founder
New Cloud Technologies, McHenry

Donna St. Germain, Director
SafeNet, Belcamp

Christopher Valentino, Director
Northrop Grumman, Millersville

Steve Walker, Founder
Informatics Coalition, Glenwood

Lisa Webb, Business Development Director
Anne Arundel Economic Development
Corporation, Annapolis

Gerald M. Whitaker, Director
Morgan State University, Baltimore

Joseph A. Whittaker, Ph.D., Dean
Morgan State University, Baltimore

Heather Wiley, Sr. H.R. Director
Sourcefire, Columbia

Maryland Higher Education Commission

Maryland Department of Information Technology

Maryland Department of Labor, Licensing & Regulation

Office of the Governor

This report's recommendations serve as an action agenda to further develop Maryland's cyber security industry. Under Governor O'Malley's leadership, the Department will work with state agencies, universities and public-private partners–including a prospective cyber security industry alliance–to realize these goals.

MARYLAND OF OPPORTUNITY.

WWW.CHOOSEMARYLAND.ORG

MARYLAND
Department of Business & Economic Development

MARTIN O'MALLEY, GOVERNOR
ANTHONY G. BROWN, LT. GOVERNOR

Printed in the USA