Cyber Mindset
Transforming education and expanding the workforce for America’s cybersecurity challenge and Maryland’s newest industry
February 2012
About the Fort Meade Alliance

The Fort Meade Alliance is a 501(c)4 non-profit independent community membership organization created to promote Fort George G. Meade, its more than 95 agencies and organizations and the surrounding areas as an economic asset, support the well being of the region with programs that support FGGM priorities, and serve as a resource to help make connections that make a difference. The Fort Meade Alliance is supported by membership dues and through a grant from the Maryland Department of Business and Economic Development.

About the Cybersecurity: Key to the Future Forum

The Fort Meade Alliance hosted its 4th annual Education and Workforce Development Forum in February 2011 to provide government and industry insight from the front lines of cyber security and identify what needs to be done by educational institutions, workforce development organizations and private industry to win the nation’s cyber security fight.

More than 250 government and industry specialists, educators and workforce development representatives gathered at the Kossiakoff Conference and Education Center at the Johns Hopkins University, Applied Physics Laboratory for “Cybersecurity: Key to the Future.”

This unprecedented event brought together the region’s most influential leaders in cyber security including Deborah Bonanni, Chief of Staff for the National Security Agency and Jenny Menna, Director for Critical Infrastructure, Cyber Protection & Awareness for the Department of Homeland Security, as well as government officials who understand the importance of our nation’s cyber security — Congressman Dutch Ruppersberger and Congressman John Sarbanes. Attendees also heard from FMA President Rosemary Budd and FMA Education & Workforce Development Chair Penny Cantwell.

The morning program was comprised of three panels of representatives from U.S. Cyber Command, NSA and DISA, as well as industry leaders from Constellation Energy, HP, Lockheed Martin, ManTech, SAIC, TASC, TeleCommunication Systems and the Federal Reserve.

The afternoon included small breakout sessions with the panelists and educators to discuss what K-12, colleges and universities and workforce development organizations can do now and in the near future to meet the cyber security challenge.

About this White Paper

This white paper was created by the Fort Meade Alliance in conjunction with the O’Ferrall Group, LLC. Forum coverage was provided by Sage Policy Group, Inc. A special thank you to Anne Arundel Public Schools for donating the printing of this white paper.

Copyright Information

Copyright 2012 Fort Meade Alliance
# Table of Contents

Cybersecurity: Key to the Future  
Executive Summary  
Charging Onto the Cyber Battlefield
  - Confronting a new threat level  
  - Building a cyber force  
  - Are certifications an aid or obstacle to building a cyber workforce?  
  - Rapid changes, immediate threats  
  - Conclusion  
Seizing a Unique Opportunity
  - In search of cyber workers  
  - Corporate training initiatives  
  - Good cyber hygiene becomes a new civic duty  
  - The challenge with security clearances  
  - Project SCOPE: Security Clearance Overview and Preparation Education  
  - Sparking interest in cyber careers  
  - Conclusion  
Imagining New Forms of Risk Management
  - Breaking the barriers of imagination  
  - Expanding public-private partnerships  
  - Confronting a new scientific challenge  
  - Conclusion  
Training the Cyber Warrior
  - A national shortage of STEM students  
  - Concerns about quality programs and foreign students  
  - Patriot hackers: Cyber experts find talent in unconventional places  
  - Inspiring a generation  
  - Developing a cyber curriculum  
  - Conclusion  
Key Recommendations and Findings  
Sponsors  
  - TASC  
  - Booz Allen Hamilton  
  - Lockheed Martin  
  - SAIC  
  - LG-TEK  
Fort Meade Alliance 5-Star Members
Since 2007, the Fort Meade Alliance has hosted annual education forums designed to probe critical issues facing our nation in the area of human capital development in our defense and homeland security sectors. By attracting top-level officials and thought leaders from government, industry and academia, these forums now rank among the forefront of discussions in Maryland regarding the challenges facing the state and the nation as we strive to create the workforce of the future.

"To date, malicious cyber activity has been directed at nearly every sector of our infrastructure and economy."

- Secretary of Defense William Lynn

Previous forums focused on K-12 education, higher education and STEM (science, technology, engineering and math) education. In 2011, however, the Fort Meade Alliance opted to focus its forum on cybersecurity — the cyber threats facing the nation, the skills needed to mount first-class cyber defense, shortages in the existing workforce, and needs and opportunities to educate a new cyber workforce. The forum — which brought together government, academia and industry leaders from such critical sectors as defense, finance, treasury and healthcare — constituted a first-of-its-kind discussion of cybersecurity in Maryland.

Defending America from cyber threats

The critical need to protect America’s cyber operations is evident. We live in a highly interconnected world whose economy is dependent on safe and secure computers, hand-held devices, networks and the Internet. According to the 2011 Department of Defense Strategy for Operating in Cyberspace, “From 2000 to 2010, Internet usage has grown from 360 million to over 2 billion people.”

The level of threat facing those cyber operations, however, is startling and sobering. Cyber attacks against individuals, businesses and governments occur at an alarming rate today. General Keith Alexander, Commander of U.S. Cyber Command and Director of the National Security Agency/Central Security Service, estimates that Pentagon computer systems alone are probed at least 250,000 times each hour. According to Deputy Secretary of Defense William Lynn, “To date, malicious cyber activity has been directed at nearly every sector of our infrastructure and economy.”

The sources of those threats range from 8th graders to spies, terrorists, nation states, hacktivists, rogue countries and industry/government insiders. And those attacks can inflict significant damage. An attack on CISCO’s supply chain impacted product integrity and cost the company millions. Hackers attacked Sony PlayStation’s online gaming system in April 2011, tapping personal information on more than 100 million account-holders worldwide and forcing Sony to suspend the online business for more than three weeks. Immediate recovery efforts cost Sony more than $171 million and executives estimated that lawsuits and lost business could eventually drive the total cost into the billions. Malicious code, which was injected through e-mail into a major defense company’s networks, caused the exfiltration of significant quantities of proprietary and classified information. Cyber attackers stole the source code for RSA ID secure tokens in March 2011, triggering a multi-million dollar recovery effort. Some cyber operator even used a simple thumb drive to penetrate Department of Defense networks.

The threat is so serious and broad reaching that the Department of Defense’s 2011 Strategy for Operating in Cyberspace expanded the military’s operational domains beyond land, sea, air and space to include the new domain of cyberspace.

What is Cyber?

Cyber is a term related to the internet, computer-managed networks, computer-managed processes and controllers, software and hardware controlled devices, software, and use of interdependent network of information technology infrastructures, and devices. Cybersecurity is prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

3. “PlayStation Network breach will cost $171 million and counting,” The Register, May 24, 2011.
Assembling an army of cyber warriors

Protecting America from this cyber threat presents the country with two daunting challenges: first, the threat itself is large, diverse and rapidly changing, and second, the United States is experiencing a severe shortage of expert and “cleared” cyber professionals.

The National Defense Industrial Association warns, “It’s pure supply and demand right now. The demand has never been higher, [and] the supply is limited... Firms are recruiting against one another.” Rep. Michael Arcuri, D, NY, said on the floor of the House that the federal government alone will need to recruit and hire up to 1,000 additional cyber workers each year to address potential threats. Currently, the Department of Defense is hiring about 80 cybersecurity professionals annually. Other federal departments and agencies are funding about 120 scholarships for students aiming to fill entry-level cyber jobs.¹

The shortage extends beyond sheer numbers. America’s cyber workforce is also suffering from a quality deficit. Alan Paller of the SANS Institute, an organization that trains system administrators and computer engineers, says schools aren’t turning out enough students with the technical know-how to defend critical networks. “This shortage is as tough as the shortage of scientific people we had in the 1950s,” Paller says. “The country has about 1,000 people that could compete in a cyber competition at a high level today. We actually need between 20,000 and 30,000.”

Forging vital partnerships

Building that workforce will require close, creative and dynamic partnerships involving government, industry and academia. Attacking the cybersecurity challenge in silos simply does not work. Government holds the authority for cyber, the mission understanding and control of the security clearance process. Industry has the innovation processes as well as many emerging technologies and professionals to tackle cyber challenges. Meanwhile, educational institutions are vital to training a cyber workforce. Together, we need to tackle the challenge of human capital development in cybersecurity.

Currently, many educational institutions lack understanding of “real life” cyber challenges and missions, and their curricula lack many elements needed in cyber education, including cyber aspects of policy-making, risk-management, law, engineering and architecture. At the same time, we are seeing too few American students focusing on STEM courses and too many American universities awarding high percentages of advanced degrees in STEM fields to foreign nationals.

By working closely together, government, industry and academia can help develop curriculum to meet real world needs and help motivate more students to study STEM subjects and pursue cyber careers. Together, we can eliminate the shortage of cyber professionals and better protect the nation.

The Fort Meade Alliance commitment

Filled with a unique concentration of federal agencies involved in cybersecurity, the Fort Meade region experiences the challenges of the cyber sector acutely. Cyber companies in our region steadily strive to find qualified individuals to fill open positions and often find that new hires need additional training to develop the requisite skills and experience to become proficient at cybersecurity work.

The Fort Meade Alliance is committed to bringing industry leaders, government officials and educators together to address this shortfall in our cyber workforce. The shortage of students in STEM and other cyber-related disciplines will require innovation, strategic partnerships and perseverance to resolve. The FMA believes we can help address that challenge through Project SCOPE, STEM Family Night, legislative changes to the security clearance process, the academic balance between American and foreign students, and other measures. We look forward to putting this paper’s recommendations into action. We are excited about the opportunities to help the country conduct vital cybersecurity work and about the Fort Meade region’s opportunity to be the epicenter of cybersecurity in America. ✨

Executive Summary

While the Fort Meade Alliance provides the oversight and program presentation for such events as our Cybersecurity: Key to the Future Forum, it is our members and regional partners, comprised of business and industry experts, educators, government agencies and workforce professionals, who help support our efforts to meet the growing demand for a highly skilled workforce in the Fort Meade region.

The focus of this white paper is to summarize the information shared during our program, key discussion points shared in the breakout groups, include current data from government and industry on cyber workforce needs and gaps, supported by relevant data to provide the FMA recommendations and establish critical programs and initiatives. These programs and initiatives will assist in providing our region with a well educated and prepared cyber workforce — a key need in establishing Maryland as the epicenter of cybersecurity for our nation.

The cybersecurity challenge that faces our public government entities as well as all private sector businesses and each of us as individuals is critical in providing security, protecting the U.S. economic base, and individual personal security. A major gap exists in the public and private sectors of a qualified and knowledgeable cyber workforce. While gathering a myriad of information on the subject, we discovered a good analogy to understand this cybersecurity.

Cybersecurity can be compared to a “teaching hospital,” with patients having the same disease but each being treated individually based on various factors. Cybersecurity is similar because each cyber threat requires a “different diagnosis and course of treatment,” analogous to a complex set of rapidly evolving diseases and patients. Only by mixing and matching a vast array of cyber approaches that require a wide-range of skills will we create the right “cure” for the cyber threat. Dr. Patrick O’Shea, at the University of Maryland, stated “the threats are enormous, yet cybersecurity as an academic enterprise is confused and ill-defined.”

After meetings with numerous industry partners and listening to our educators to better understand their plans to provide cybersecurity curriculum, the Fort Meade Alliance felt our region would benefit from industry and government agency expertise to understand the challenges and gaps of what is needed and how to create a cybersecurity “ready” workforce. In our planning meeting, where we utilized the experience of industry leaders in the region, talking points were formulated to be discussed during our cyber education forum. These industry leaders shared their experiences with skill gaps in new employees, inability to hire qualified candidates for currently open cybersecurity jobs, inability to find candidates eligible for obtaining security clearances, as well as candidate weaknesses in several areas of professional skill sets: critical thinking, writing, and oral communication. During this meeting, these cybersecurity leaders quickly discovered they had very similar concerns, expressing that new hires are inadequately prepared and are not ready to be placed on cyber projects without additional and sometimes intensive training provided by the employer.

At the cyber education forum, the Fort Meade Alliance brought together cyber leaders from government, industry government contractors base, and commercial industries in panel discussions to provide insight of relevant workplace and operational based information, from their vast experience in this field, which we will use to help establish innovative curriculum in this area. We feel that industry involvement in the development of curriculum pathways for Maryland students will enhance success for both the student, provide up-to-date industry relevance and help meet our economic needs.

In three afternoon breakout sessions, the Fort Meade Alliance gained insight from groups comprised of K-12, colleges, universities and workforce professionals, partnering each group with industry and government support teams, to share ideas for the development of relevant cyber skills. The Fort Meade Alliance is using the information shared at the event, supported by industry information gathered on the subject of cybersecurity education and training, to develop initiatives that support the workforce needs in Maryland and create relevant cybersecurity curriculums which we hope can become a model for the nation in creating critically needed cyber workforce.

This white paper provides a comprehensive overview of the information shared during the event, offers a wealth of knowledge and insight into the fast-paced cybersecurity domain and the challenges that exist today. This paper has captured the myriad of rich expertise offered by the panelists, further enriched with relevant industry data and expertise, offering a unique glimpse into a largely uncharted and newly developing area for future curriculum opportunities.

The Fort Meade Alliance is especially interested in...
several key points identified in this white paper from remarks made during the forum, as well as research conducted to support these findings.

1) While it has long been recognized that there is a critical shortage of STEM professionals in our colleges, the data clearly indicates that the strong foreign student population is a factor in preventing U.S. students from obtaining entry for STEM degrees.

2) The skill sets need to be defined, which is currently being completed, and having this quantified will provide a more accurate understanding of what coursework needs to be included in cybersecurity training.

3) Concern expressed by all panelists with current cybersecurity curriculum at our colleges and universities is that the scope of study must broaden to include “intangible” skills such as risk management, policy, communication, leadership and other critical professional needs which are lacking in most new hires in this field.

4) Additionally, the panelists all point out that while foreign cyber threats are a grave concern, the largest threat is internal. This would strongly suggest compliance training programs and education for the American business workforce, which would also support good online protocol.

5) The last major point is one that has been stressed repeatedly in our region and is highlighted in every education forum hosted by the Fort Meade Alliance and this is the critical need to grow the STEM pipeline for today’s students. This will take a major effort by everyone, including industry, government, educators, community and workforce to dedicate significant resources to insure our students today become our STEM resources tomorrow. Immediate change is needed to turn the tide toward STEM and developing the cybersecurity workforce.

Lastly, there is an issue that continues to be raised regarding security clearances in our workforce. While the process and time to obtain a security clearance has made progress, the significant number of foreign students in our colleges and universities for STEM degrees not only cannot qualify for a security clearance, but in many cases these students are returning to their native country and using the skills taught in American colleges for achievements in those foreign countries — to the detriment of the United States. The Fort Meade Alliance continues to struggle with how this situation in our colleges and universities of allowing such a large foreign national student population in our STEM degree programs benefits the U.S. and addresses the critical gap and need to increase STEM students for our workforce pipeline. We wonder when the issue will become important enough to our nation that we begin to turn the tide in favor of greater opportunities for U.S. students.

We hope this white paper will contribute to enhance the education and workforce needs for our region and that our efforts support the creation of the best trained cybersecurity workforce in the country. The Fort Meade Alliance initiatives, developed based on some of the issues identified in this white paper, are planned to meet industry identified requirements and we look forward to having our combined efforts make a significant difference for our region and the nation.

The Fort Meade Alliance is excited to be part of the cybersecurity future in Maryland and we look forward to working across the public government, private businesses, workforce and education partners in the creation of innovative initiatives to set and achieve a new benchmark for education partnerships.

Rosemary Budd  
President  
Fort Meade Alliance

Penny Cantwell  
Chair Education and Workforce Development  
Fort Meade Alliance

Deon Viergutz  
President-Elect  
Fort Meade Alliance
It's a battlefield that nobody can see or set foot on. Yet cyberspace has become a highly contested space, packed with opportunities and peppered with hazards, threats and a rapidly evolving barrage of outright attacks. Government, industry and academia have taken major steps to address these emerging threats. The high speed of technology adoption and the relentless development of more sophisticated attacks have left many agencies and companies scrambling to quickly develop security measures while also identifying a full roster of essential cyber skills and developing a top-flight cyber workforce.

Confronting a new threat level

Hundreds of thousands of times every day, computer networks across America become the target of cyber threats. The sources of those threats range from hostile states and other enemies seeking to do significant harm to hacktivists, like Wikileaks, digging for confidential information. They include criminals in search of profit, hackers eager to defeat encryption codes, disgruntled insiders seeking revenge, professionals engaging in corporate espionage, and naive or careless individuals who leave a database or home network vulnerable by failing to safeguard a password or employ simple encryption.

U.S. Army General Keith Alexander, Commander of U.S. Cyber Command, has reported that the security threat to Department of Defense networks involves as many as 250,000 “probes and scans” an hour.¹

A report by the Center for Strategic and International Studies warns:

“Military and nuclear energy systems are under continuous attack, experiencing large losses. For at least the past six years, the U.S. Department of Defense, nuclear laboratory sites and other sensitive U.S. civilian government sites have been deeply penetrated multiple times by other nation states. China has downloaded 10 to 20 terabytes of data from NIPRNet (the sensitive, but unclassified U.S. military network)..."

“Terrorists and organized crime groups are actively exploiting weak U.S. security and extorting money used for criminal purposes and to buy terrorist bombs. In October 2008, for example, Express Scripts, one of the nation’s largest processors of pharmacy prescriptions, reported extortionists had threatened to disclose personal and medical information on millions of Americans if the company failed to meet payment demands.”²

At the Fort Meade Alliance’s Cybersecurity: Key to the Future Forum, Charles Croom — U.S. Air Force Lieutenant General (Retired), former Director of the Defense Information Systems Agency and current Vice President of Cybersecurity Solutions for Lockheed Martin Information Systems and Global Services — said 2010 provided ample insights on the scope and intensity of cyber threats facing the world.

“We keep asking ourselves, ‘When is the 9/11 [cyber attack] going to happen?’ Well, the 9/11 has occurred at least a number of times,” Croom said. “Last year, 2010, CISCO publicly came out and said, ‘We had a penetration into our supply system and we are using counterfeit parts.’ The Deputy Secretary of Defense came out and said, ‘Our classified network was broken into through the use of a thumb drive.’ Google — perhaps the largest IT company, clearly with plenty of talent and smarts in this area — publicly asked the government for help as they faced an intrusion from China.”

And then there was Stuxnet. Discovered in July
2010, the computer worm spread indiscriminately but targeted its attacks on a Siemens software product that controls, monitors and gathers data from the operations of certain heavy industrial equipment. In particular, Stuxnet targeted five Iranian organizations in an apparent effort to undermine that country’s uranium enrichment infrastructure. Western media reported that the worm impaired operations of Iran’s centrifuges.

“I think it even surprised us in the business at how sophisticated this particular penetration was against a system that was apparently isolated from the network, attacking a particular piece of equipment and hiding its attack for a number of months and doing great damage,” Croom said.

It is impossible to tally the exact costs of all cyber attacks over the course of a year, yet cybersecurity experts predict those costs are enormous. In November 2011, Business Insider reported that some industry analysts have estimated that traditional data theft costs U.S. governments and corporations as much as $1 trillion annually in information losses.

Joseph Pacileo — U.S. Army Colonel (Retired) with 25 years experience in military intelligence and the current Vice President of Cyber Operations at ManTech International Corporation — cautioned at the Cybersecurity Forum that the largest and most costly data security threat facing most organizations is employees who have full access to the organization’s core servers.

In March 2011, Ponemon Institute LLC, an information security research group, released its annual report on cybersecurity. The report concluded that negligent employees remain the leading threat to data security and accounted for 41 percent of all data breaches in 2010. Malicious cyber attacks, however, also rose in 2010 to 31 percent of all data breaches — up 7 percent from the previous year. The average cost of data breaches also rose for the fifth consecutive year. In 2010, the average cost of a single data breach reached $7.2 million or $214 per compromised record, and about 85 percent of all U.S. companies had experienced one or more data breaches in the past.

Events in 2011 — such as the attack on Sony’s online...
gaming network that compromised the personal data attached to 100 million accounts, forced a 23-day shutdown of the gaming service and cost Sony more than $171 million — demonstrated that the cost of cyber attacks is escalating quickly.

“The threats are serious,” said U.S. Air Force Col. George Lamont, Director of Exercise and Training for U.S. Cyber Command and an FMA Forum Panelist. “To appropriately deal with them will require a common vision, unity of effort and dedicated resources. No single organization can solve the cybersecurity challenges that face us. Thus, it is crucial to bring all of the players together. This is a team sport.”

Air Force Maj. Gen. David N. Senty, the first Chief of Staff of U.S. Cyber Command, told the American Forces Press Service in September 2011 that effective cyber defense not only has to be a team sport, but one in which players rapidly and expertly adapt to changing conditions. The press service wrote:

Facing off against this [cyber] threat is a force Senty compared to a soccer team. Unlike a football team that has distinct offensive and defensive players, he said, the cyber force must adopt the rules of soccer, conducting “continuous play, with offensive and defensive [skills] at all times,” operating and defending in the same cyberspace. “That sort of mindset was part of bringing the command together,” he said.¹

“"No single organization can solve the cybersecurity challenges that face us. Thus, it is crucial to bring all of the players together. This is a team sport." — Col. George Lamont, U.S. Cyber Command

Building a cyber workforce

The rising frequency and sophistication of attacks on our cyber infrastructure have increasingly drawn the attention — and the concern — of government, industry, academia and the public. In recent years, the President of the United States has initiated measures raising cybersecurity to a national priority and issued cyber directives to the Department of Homeland Security and the Department of Defense.

In May 2010, the Secretary of Defense activated the U.S. Cyber Command to coordinate American response to cyber threats. The new command, which was formed through the integration of cyber units from all services of the military, was tasked with defending Department of Defense information networks as well as enabling the department to conduct full-spectrum cyberspace operations. Headquartered at Fort George G. Meade, U.S. Cyber Command works closely with other federal agencies tasked with cyber missions, including the National Security Agency, the Defense Information Systems Agency and the Department of Homeland Security. Consequently, the Fort Meade region is quickly becoming an epicenter of cybersecurity as those agencies embark on a myriad of cyber initiatives.

The rapid emergence of this new, digital battlefield has presented federal agencies with considerable challenges, speakers at the Cybersecurity: Key to the Future Forum stressed.

A primary challenge is to determine what kinds of professionals will be needed to defend American cyberspace and execute cyber missions, and then to train and recruit those professionals. “This is such a hard problem, it takes many talents and disciplines to get our arms around it,” Croom said.

Several other Forum speakers stressed that America’s cyber workforce will need not only skilled engineers, computer scientists, mathematicians and other scientists, but also linguists, intelligence analysts, business experts and others.

Col. Lamont explained that his work — and the work of numerous other high-level federal officials — currently revolves around two main goals: identifying all training requirements for the federal cyber workforce and helping U.S. Cyber Command deliver trained, ready professionals to all mission commanders.

The cyber industry itself has not yet established a standard, unified set of cyber certification requirements or curriculum standards. For its part, the Office of the Secretary of Defense is conducting a study to identify all roles, functions and skills of a cyber workforce as well as DoD’s ability to fill all those positions, Lamont said.

Meanwhile the NSA is conducting extensive analysis to map those workforce roles based on existing Knowledge, Skills and Abilities (KSAs). The agency is analyzing existing Cyber Command workforce training programs to determine how closely they match those KSA requirements for cyber workers and to help fine tune training programs to generate essential professional skills. The NSA is also raising its own workforce training and certification standards to meet DoD guidelines.

To date, several Fort Meade agencies have experienced great success in attracting talented cyber professionals, forum speakers said. In the midst of its move to Fort Meade, DISA increased its cyber workforce by more than 70 percent and succeeded in attracting talented and diverse new cyber employees, said Mark Orndorff, Director of DISA’s Program Executive Office for Information Assurance and NetOps and an FMA Forum Panelist. NSA which is expected to hire 1,800 new employees in 2011, steadily attracts highly qualified applicants from across the country, including several thousand more each year than the agency can hire, said Deborah Bonanni, Chief of Staff for the NSA.

Federal officials and industry watchers, however, warn that the U.S. government overall is consistently falling short in hiring and retaining cyber professionals. And that shortfall could grow more severe in coming years as cyber needs continue to grow.

In 2009, the Department of Homeland Security announced plans to hire 1,000 cybersecurity experts. However, during a 2011 hearing of the House Homeland Security Committee, Philip R. Reitinger, Deputy Undersecretary for the National Protection and Programs Directorate, said that DHS had added just 260 new cyber personnel. The department is now aiming to hire 400 cybersecurity professionals by October 2012.¹

Larry McKee and Jim Crouch of the National Security Cyberspace Institute warn that “the U.S. Government continues to fall short in recruiting and

Are Certifications an Aid or Obstacle to Building a Cyber Workforce?

Certifications are used in many professions, and they would enable federal agencies to establish baseline qualifications for its cyber workers and even map out career paths for those professionals. By requiring an individual to complete intensive education, engage in hands-on experience and pass an examination, a certification can ensure that an individual has deep knowledge of a particular technology or skill. But is certification the best way to develop a capable cyber workforce.

The Cyberspace Education and Training, a publication by the National Security Cyberspace Institute, points out that “the certification issue has sparked debate about its purpose and value. Although a good certification standard might be a measure of a baseline level of competence, it is not an indicator of job performance.”

The report questions whether certifications could keep pace with rapid changes in the cyber field. It quotes Daniel Castro, a senior analyst at the Information Technology and Innovation Foundation, as saying: “Certainly more workforce training, although not a panacea, can help teach workers how to respond to known cyber attacks. However, workforce training is not certification, and organizations, not Congress, are in the best position to determine the most appropriate and effective training for their workers.”

The Armed Forces Journal in February 2011 suggested that certifications might even hinder federal efforts to assemble a large and innovative cyber workforce: Certifications ensure that an individual has had recognizable and measurable cyberspace security training and exposure to information technologies and techniques common to cyberspace operations/missions. However, a drawback to this method is that it limits the available pool of immediate and potential candidates and can lead to difficulties hiring fully capable but uncertified personnel. An overreliance on certifications prevents many otherwise capable personnel from participating in critical federal cyberspace-domain operations. It also tends to favor personnel who are good at test-taking, as opposed to those who do not have that talent but are good at practical application of cyberspace skills and experience. These certifications do not judge the ability of the test-taker to apply critical and innovative thinking skills to cyberspace-domain security missions.²

² “U.S. cybersecurity must-do’s,” Armed Forces Journal, February 2011. (sidebar)
retaining information technology professionals to meet
our expanding requirements. Even with a 57 percent
increase in federal IT workforce over the past eight
years, hiring gaps still exist, primarily because of three
factors: (1) a dramatic increase in our dependency
on technology to deliver goods and services; (2) the
current and impending retirements of members of the
Baby Boom generation; and (3) declining interest by
U.S. students in the science, math, technology and
engineering disciplines.”

This problem is compounded by the current lack of
professional criteria and certification standards for
cyber professionals. This gap in workforce planning is
rendering some college training programs inadequate
to meet federal cyber needs.

A “Cyberspace Education and Training” report by the
National Security Cyberspace Institute cited multiple
causes for federal shortfalls in cyber hiring:

“Along with the other federal departments,
DoD has been unable to fill its requirement for
experienced information assurance professionals,
primarily because of the huge unmet need for
training. There are not uniform, government-wide
certification standards and no federal career path
for cybersecurity specialists. There is insufficient
training for workers to upgrade skills, inadequately
funded federal scholarship programs to lay a
foundation for a talent pipeline, a cumbersome
and lengthy federal hiring process, and a lack of
in-house capability at many agencies to properly
manage contractors. To date, no one in the
government has been tasked with assessing the
cybersecurity workforce, how many people will be
needed across the federal system in the short-
and long-term, what skills are necessary and how
top talent will be obtained...

“A comprehensive, integrated strategy is needed
to overcome the talent deficit. The administration
must assess its short- and long-term workforce
needs, develop a government-wide blueprint to
recruit, hire and retain top cybersecurity talent,
and then aggressively implement it. The plan
should provide guidance on the appropriate
roles for civil servants and private contractors.
Government should lead a campaign to encourage
universities to offer, and students to pursue,
cybersecurity education programs.”

The Fort Meade region which has quickly become a
national center for cyber activity, could feel those
staffing shortages acutely.

Bonanni said she is concerned that the “historic
confluence of events” — retirements by Baby Boomers,
growing demand for cyber workers and low rates of
American students specializing in STEM — will create
a shortage of cyber workers in the future that will
amount to a “national security crisis.”

The NSA and other agencies are already expanding
internship programs plus outreach efforts to schools,
universities and the community in order to excite more
students and workers about STEM studies and careers
in cybersecurity.

2. ibid
Rapid changes, immediate threats

As U.S. Cyber Command, NSA, DISA and other federal agencies, as well as all the supporting contractors in the private industry, work to build an expert, cyber workforce, they must also address immediate and critical cyber issues.

George “Dennis” Bartko, Chief of the National Security Agency’s Cyber Task Force and a Special Assistant to the Director of the NSA’s Comprehensive National Cybersecurity Initiative, told attendees at the Cybersecurity Forum, “Cyberspace changes so quickly. It is never really the same for very long.” The nature of cyber attacks changes rapidly, so that new days bring new types of threats, Bartko added.

“Because it is a continually changing domain with really, really important challenges and opportunities, we can’t sit back and wait for the ideal solution and then move forward,” he said. “We strongly believe from our experience that you have to learn by doing and continually change and improve.”

At the Defense Information Systems Agency, leaders in cybersecurity are pursuing three avenues of establishing effective cyber defense: adopting solutions from other agencies, buying solutions from the private sector or creating solutions themselves. Orndorff said that means the agency’s workforce increasingly must include both acquisitions professionals and engineers who are experts in cyber. In addition, DISA will need to recruit cyber engineers who are able to develop or acquire effective cyber solutions, customize them to a myriad of systems operated by different agencies within the Department of Defense, and train other staff to use those tools effectively. DISA, which is striving to create a larger and better informed cyber workforce by engaging students as part-time workers and interns, is aiming to eventually draw 10 percent of its workforce from graduating interns.

Meanwhile, the Department of Homeland Security is involved in a myriad of efforts to advance cybersecurity throughout federal agencies and public services. They include creating Einstein 2 and piloting Einstein 3 to observe network traffic on federal agencies’ networks and detect intrusions and malicious activity; supporting the Volpe National Transportation Systems Center in efforts to enhance cybersecurity for transportation infrastructure; and supporting the Department of Energy’s Idaho National Laboratory in a multi-year cybersecurity program designed to protect electrical power grids, oil and gas refineries, telecommunications systems and other critical infrastructure.

Throughout federal agencies, officials stress that government and the private sector must work closely together to understand the rapidly changing cyber field, develop professional standards and adequate work force, and deliver essential cybersecurity to the country. In Defending a New Domain, William Lynn, III, Deputy Secretary of the Department of Defense, states the consolidation of cyber defense capabilities from multiple DoD agencies and the government’s signals intelligence operations into U.S. Cyber Command was a powerful step in strengthening America’s cybersecurity. Now, U.S. Cyber Command and the Department of Homeland Security work “closely with private industry to share information about threats and to address shared vulnerabilities,” Lynn wrote.

In a 2011 article in National Defense Magazine, Robert Giesler, senior vice president for cyber programs at SAIC, said a balance between cyber talent in the public and private sectors is important for America’s cybersecurity. The federal government, he said, is “recognizing that a healthy mix of a trained federal work force is critical but you’re never going to be able to solve the cyber problem with just an in-sourced federal work force. It’s got to be a very healthy, dynamic balance between federal employees and contracting work force to address such a dynamic threat. I think we’re reaching equilibrium.”

Reflecting on the way that U.S. Cyber Command has been evaluating America’s future needs for a cyber workforce, Maj. Gen. Senty said that he expects the command to work “with the service components to develop a common mindset, common training standards

---

and career progression across the components. Senty said he envisions a ‘very deliberate rotation schedule’ of assignments in the future between Cyber Command, its service components and combatant commands to ensure a solid experience base in building networks, defending networks and operating in cyberspace,” the American Forces Press Service reported.¹

Numerous speakers at the Cybersecurity Forum stressed that such multi-level information sharing must continue and expand among government, industry and academia in order to master the rapidly evolving challenges of the cyber realm. Experts in the cyber industry and the academic field need to form an alliance to continually update each other about evolving workforce needs and new opportunities to integrate those needs into curriculum.

Conclusion

Legions of cyber attacks, information leaks and computing carelessness have presented the United States with both a major threat to national security and a vast, diverse need for new breeds of cyber professionals. Some federal agencies, such as the National Security Agency and the Defense Information Systems Agency, have made admirable strides in assembling this leading edge workforce. But overall, the federal government is regularly falling short of cyber hiring goals.

Several key factors are contributing to this shortfall:

- A shortage of U.S. citizens pursuing degrees in STEM fields;
- Even graduates from good universities have an absence of a comprehensive analysis of the professional expertise needed to complete all cyber duties, requiring extra training upon hiring;
- Rapid changes in cyber threats that require cybersecurity agencies to frequently develop new skills;
- Lack of identified certification standards and training programs specifically tailored to federal cyber needs; and
- Unavailability of a federal blueprint for how to train, recruit and retain top cyber talent.

Presentations at the Fort Meade Alliance’s Cybersecurity forum stressed that public-private partnerships as well as strong, dynamic partnerships between the cyber industry and academia could greatly help the federal government satisfy its needs for better training, an expanded workforce and new technologies in the cybersecurity field. They also stressed that:

- The cyber battlefield is everywhere — inside and outside the business, agency and home — and we have no clearly defined defense;
- A shortage of skilled, trained workers in STEM/cybersecurity is acute and critical, resulting in severe competition for workers and a need to provide additional, on-the-job training to new hires; and
- While the need to define skills and certifications for cybersecurity is critical, the cybersecurity industry also requires more intangible skills such as innovative thinking, creativity, communication and leadership — which are difficult to quantify for educators.

Seizing a Unique Opportunity
Maryland stands to be the epicenter of cyber in America, but it must assemble a leading edge workforce

“Maryland companies and organizations are optimistic about the continued growth of cybersecurity efforts, specifically the unprecedented opportunities in 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 could obtain security clearances — as the state’s most immediate and significant challenge.”
~ “Cyber Maryland,” Maryland Department of Business and Economic Development

In corporate America, cyber opportunities, challenges and unavoidable needs are growing at a dizzying pace. There are opportunities to master and profit from the rapidly emerging and vitally important field of cybersecurity. There are ample new prospects for government contracts. Federal agencies continually stress that a vigorous partnership with the private sector is vital to building America’s cyber expertise, generating maximum benefits and efficiencies from all cyber budgets, and ultimately securing all of America’s computer networks — government, business and critical infrastructure. At the same time, electric utilities, communications networks, banks, retailers, power plants, media companies and countless other enterprises are striving to build their own cyber defenses and looking to contract with cyber experts.

Cyber Maryland, a report by the Maryland Department of

Global spending on cybersecurity
Spending by federal agencies and federal contractors on Information Technology and Information Security products and services has been growing at a robust rate and is expected to keep climbing.

![Bar chart showing IT and IS expenditures in billions from 2008 to 2013 and 2009 to 2014.](chart)

Source: INPUT, a market research firm
Business and Economic Development (DBED), concluded that “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 cybersecurity products and services, the report added, is expected to surpass the federal market.1

Maryland, which already has a critical mass of federal agencies involved in cybersecurity, has a unique opportunity to be the epicenter of cyber in America. With the fifth largest concentration of IT workers in the country and the second largest concentration of custom computer programmers, the state’s business sector is primed to seize that opportunity.2

Furthermore, the private sector benefits of developing a cyber hub in Maryland would extend beyond large high-tech firms to numerous small businesses. According to Cyber Maryland, “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.”3

Maryland’s efforts to grow its cyber industry, however, face one sweeping challenge, according to Cyber Maryland. “Overwhelmingly, stakeholders reported a need for more qualified workers — particularly those who could obtain security clearances — as the state’s most immediate and significant challenge.”

So how will Maryland companies deliver the myriad experts, extensive staff, training programs and public outreach efforts that will be needed to satisfy their clients’ cybersecurity needs? Undoubtedly, the need for expansive and leading-edge cyber expertise will be felt across the country, but it will be felt acutely in the Fort Meade region.

In search of cyber workers

Maryland already has a vigorous technology sector. However, as the Fort Meade region strives to serve as a national center for cybersecurity, the number of technology positions — and the need for technology experts — will mushroom.

After the Secretary of Defense announced the creation of U.S. Cyber Command, Pentagon officials estimated that 1,000 personnel would work at Cyber Command’s headquarters in Fort Meade and that the command would eventually require more than 21,000 military and civilian workers. That’s both an enormous opportunity and a daunting challenge for local companies that serve America’s intelligence, military and homeland security communities.

Richard (Dick) Bowers, Vice President of Cyber Services at TASC and a Forum Panelist, noted that the private sector is already having difficulty attracting sufficient individuals with science, technology, engineering and mathematics (STEM) expertise. Not only are universities graduating too few Americans in STEM disciplines, but many of those graduates are bypassing the cyber industry and opting to take jobs on Wall Street or in other professions which offer attractive salaries, don’t require security clearances and are often better understood by the general public.

In addition, many STEM graduates lack core skills — technical and non-technical skills — that are essential in the cyber field, speakers at the Cybersecurity Forum said. Those skills include core knowledge of computer languages as well as problem-solving, creative thinking, communication and leadership abilities.

Speakers at the Cybersecurity: Key to the Future Forum noted that some computer science graduates have ample courses and even certifications in software products and operating systems, including elite systems such as Java. Yet those same graduates sometimes lack fundamental knowledge of core computer languages, such as C++ and assembly languages, and that knowledge is essential to mounting thorough cyber defenses.

Some of America’s STEM graduates are unable to fill jobs in America’s cyber field because they are foreign nationals and unable to obtain security clearances. A study by Compete America, The Alliance for a Competitive Workforce, concludes that 42 percent of all master’s degrees in engineering and 53 percent of all PhDs in engineering awarded by American universities go to foreign students. Among Maryland colleges and universities, foreign students receive 23 percent of engineering master’s degrees and 53 percent of engineering PhDs. (For a complete list of all states, see the chart on page 24).

The report concludes: “It is counterproductive for the United States to train foreign scientists and engineers

2. ibid
3. ibid
in our colleges and universities and then send them home to compete against American businesses. The U.S. visa system for highly educated professionals must be permanently fixed so that America can retain those talented minds for U.S. economic growth and job creation.”

Speakers at the FMA’s Cybersecurity Forum said that American universities need to ensure there are adequate seats in advanced degree programs to accommodate qualified U.S. citizens who are also capable of obtaining security clearances. They also noted that industry often snaps up graduates of four-year STEM degree programs then funnels them into higher education programs within the company. Consequently, those individuals don’t complete master’s degrees or PhDs at American universities.

Other STEM students and professionals lack essential, non-technical skills, forum speakers said.

“Our interns come in with such incredible engineering and science skills, and if there is anything we could put more emphasis on in moving forward it would be expanding their ability to communicate and lead, especially outside of people who are as smart as they are,” said Mark Orndorff, Director of the Executive Office for Information Assurance and NetOps at the Defense Information Systems Agency. “I have this little math formula in my head. It seems to me that your effectiveness is dependent on your abilities multiplied by your ability to communicate and then applied to some exponential factor which is your ability to lead. The engineer who can talk to people who aren’t engineers that is a rare individual who is key to the future of our organization.”

Howard Clifford, a Hewlett Packard Distinguished Technologist and the company’s Chief Technologist for the U.S. Intelligence Community focusing on cybersecurity, said at the FMA Cybersecurity Forum that HP sees a skill gap even in some highly educated

It is very hard to find people with very, very rigorous backgrounds. Even people coming to us with degrees in computer science with a lot of coursework in languages and operating systems and the use of computers don’t seem to have the rigorous background of analytical skills and critical thinking skills. If there is one thing that I would give as feedback to universities and education systems it is to really focus on critical thinking and analysis skills.

- Howard Clifford, Chief Technologist, Hewlett Packard

computer scientists. “It is very hard to find people with very, very rigorous backgrounds. Even people coming to us with degrees in computer science with a lot of coursework in languages and operating systems and the use of computers don’t seem to have the rigorous background of analytical skills and critical thinking skills. If there is one thing that I would give as feedback to universities and education systems it is to really focus on critical thinking and analysis skills.”

Corporate training initiatives

Those shortages of cyber professionals — both in quantity and in quality — have compelled some companies to initiate their own efforts to attract and properly train cyber professionals.

Those initiatives include a range of efforts to train existing technology workers to handle cybersecurity work, as well as such soft skills as teamwork, communication, leadership and creativity. Companies are developing or enrolling employees in intensive, three-month, cyber development courses and other training programs. Executives say those courses can be costly for the company and demanding on the employee. However, they can convert a core computer scientist into a cybersecurity professional, said Joseph Pacileo, Vice President of Cyber Operations for ManTech International Corporation.

Companies are finding it necessary to train their employees in cyber. For instance one corporation spent $250,000 one year to train 150 employees with a comprehensive cyber program.

Robert Giesler, Senior Vice President for Cyber Programs at SAIC and Forum Panelist, said his company has experienced difficulties of finding cyber technicians as well as challenges with finding employees in intensive, three-month, cyber development courses and other training programs. Executives say those courses can be costly for the company and demanding on the employee. However, they can convert a core computer scientist into a cybersecurity professional, said Joseph Pacileo, Vice President of Cyber Operations for ManTech International Corporation.

Consequently, SAIC has adopted a three-tiered strategy for turning existing employees into cyber professionals. The tiers include a certification process, a cyber warrior track training program, and the establishment of three master’s programs from three universities on the SAIC campus. Currently, more than 100 SAIC employees are enrolled in those master’s degree programs in cybersecurity and information assurance.

Forum Panelist Andre Gudger, then-Senior Vice President of the Cyber Intelligence Group at Telecommunications Systems, Inc., said the company initiated a large cyber training program after growing dissatisfied with standard exams that certify IT professionals as adept in various products and systems. The multiple-choice exams, Gudger said, force IT staff to learn how to pass the exams while not necessarily instilling deep technical knowledge or vital problem-solving skills.

TCS Intelligence Group executives, he said, decided that “we wanted to shy away from the ‘check the box’ certifications where people can study how to take the test but still not learn anything.”

Instead, the TCS Intelligence Group established an internal training program which certifies that a staff member is proficient in an IT or cyber application only after they have been given an open-ended problem and used that application to develop a real-world, effective solution. The training and testing process produces the depth of technical expertise and the sharp creative thinking that is vital to effective cybersecurity.

“In many ways, cybersecurity is similar to 19th century medicine – a growing field dealing with real threats with lots of self-taught practitioners, only some of whom know what they are doing.”

- Center for Strategic International Studies

“A Human Capital Crisis in Cybersecurity,” a paper by the Center for Strategic International Studies, argues that the existing certification system for technology professionals does not yet meet the rapidly changing needs of the emerging field of cybersecurity:

In many cases, cybersecurity is similar to 19th century medicine — a growing field dealing with real threats with lots of self-taught practitioners, only some of whom know what they are doing. The evolution of the practice of medicine mandated different skills and specialties coupled with qualifications and assessments. In medicine, we now have accreditation standards and professional certifications by specialty. We can afford nothing less in the world of cybersecurity. We need to develop a culture of professionalism and goal orientation for the cybersecurity workforce; doing so will help prevent, detect, and/or respond to intentional or unintentional compromises involving both federal and other critical infrastructure systems.¹

Despite all the fears about hostile states and wily hackers, the single biggest threat to America's cybersecurity is the average American worker.

About 80 percent of all cyber issues are triggered by a heedless action of a worker who hasn't been properly educated about cyber hygiene, said Col. George Lamont, USAF, Director of Exercise and Training for U.S. Cyber Command.

According to PandaLabs, computer users receive 50,000 new samples of malware every day and nearly 60 percent of all consumers have experienced a computer virus. The CSI Computer Crime and Security Survey concluded that dealing with compromised computers costs nearly $350,000 per organization. Deloitte's 2010 CyberSecurity Watch Survey and a study by Carnegie Mellon University concluded that 33 percent of the most costly and damaging cyber breaches were caused by insiders.

"As a large enterprise at SAIC Global Networks with 45,000 employees, our largest threat factor is our employees and their behavior," said Robert Giesler, Senior Vice President for Cyber Programs at SAIC. "What are we doing to reach our employee base who every day when they get online are effectively holding a gun? What are we doing to tell them how to handle that gun safely so that they don't do damage to the network and the data on that network?"

A 2011 article in National Defense Magazine noted that a company's work force is often a hacker's first point of attack. Hackers send unique emails to employees prompting them to link to damaging URLs. Consequently, investing small amounts in training staff often delivers the biggest cybersecurity benefits.

Speakers at the FMA's Cybersecurity Forum stressed that American workers in all sectors, at all levels need to be better educated in good cyber hygiene – the actions that computer users can take to improve their cybersecurity, better protect themselves online and also protect their employers' networks.

Those actions can be very simple, but very powerful things, such as switching passwords from default settings, choosing passwords that aren't easily guessed, not clicking through on phishing emails, using good security software programs, and keeping operating systems up-to-date.

Information Assurance — measures designed to ensure the confidentiality, control, integrity, authenticity, availability and utility of information and information systems — is also key to cybersecurity and needs to become a greater part of day-to-day practices of American workers and network administrators.

While Information Assurance is a critical component of cybersecurity, it is only one of many skill sets and technical programs necessary to be an effective cyber warrior.

"People use information assurance interchangeably with cybersecurity, but they are not the same," said Andre Gudger, then-Senior Vice President of Telecommunications Systems Inc. responsible for the company's cyber intelligence group. "Historically, information security is the mother of information assurance."

Speakers stressed that companies, organizations and government agencies in all fields as well as educational institutions right down to grade schools need to devote energy and time to teaching basic, safe computing practices. Those simple practices, they said, could greatly improve America's cybersecurity.

"We could take care of a lot of our issues from a cyber space security perspective if we just do some of those hygiene type things versus focusing on that 10 percent [of cybersecurity] that is the super, 500-pound brain kind of activity," Col. Lamont concluded.

“Cyberspace Education and Training,” a report by the National Security Cyberspace Institute, outlined the extensive, internal training initiatives undertaken by Lockheed Martin:

“In the private sector, Lockheed Martin has a talent management strategy to support cybersecurity workforce demands. The cyber profession begins with talent sourcing and recruitment and continues with certification, training, and mentoring to move professionals along an established career track. Lockheed Martin has also created a Cyber University, which facilitates training and certification using a blended delivery approach from instructional-led training to professional study groups, lunch-time seminars, and communities of practice.

Current and new employees are able to leverage cybersecurity training and education to include CISSP certification, Security +, and technology training from Lockheed Martin Cybersecurity Alliance Partners, CISCO and McAfee.”

Northrop Grumman has created its own internal Cyber Academy. In the August 2011 issue of National Defense Magazine, Northrop Grumman’s Chief Technology Officer Robert Brammer said all of the company’s employees need basic cybersecurity skills. Northrop Grumman, which sends more than 1,000 employees a year to its Cyber Academy, requires all employees to know how to use the company’s access management system, how to protect their identities, and how to recognize malware, phishing attempts and other threats.

“Cybersecurity is not only about computer science and PCs and technical aspects like that, but it really is a much broader issue,” Brammer said.

Richard (Dick) Bowers, Vice President of Cyber Services at TASC and Forum Panelist, notes that government contractors face an additional challenge in amassing adequate cyber staff. Once a company finds a cyber professional with the right technical and communications skills, the company then has to convince “our customers” that the employee warrants a security clearance. The process of obtaining a clearance seems to be getting more difficult each year, he added.

Government contractors who must often operate on thin margins requested by government agencies, generally don’t have the luxury of funnealing extra employees into the security clearance process in case they are needed on future contracts. Speakers at the Cybersecurity Forum noted that having a bench of cleared cyber professionals would greatly enhance their ability to compete for federal contracts and quickly respond to federal cyber needs.

Some studies indicate that the security clearance process has improved in recent years. In 2010, the General Accounting Office (GAO) removed the security clearance process from its list of government procedures that faced elevated risk of experiencing inefficiencies. According to the GAO’s High-risk Series update, the DoD has reduced the average time it takes to process 90 percent of initial security clearances for industry personnel from 129 days in 2008 to 63 days in fiscal year 2010. According to the Intelligence Reform and Terrorism Prevention Act (IRTPA) Title III 2010 Annual Report released in February 2011, the average government security clearance took just 53 days to process in 2010, exceeding the IRTPA standard of 60 days required for 90 percent of all applications. In 2006, the average processing time for initial security clearances was 165 days.

Speakers at the Cybersecurity Forum stressed that several programs could help alleviate the shortage of cleared professionals in the future. They include: internship programs with key federal agencies that not only give young people exposure to government operations but also put them on a path to obtaining security clearances; initiatives in some universities and colleges to help students obtain security clearances by the time they graduate; and the Fort Meade Alliance’s Project SCOPE that creates awareness among students as young as middle school about the process and importance of keeping a clean record and

2. Intelligence Reform and Terrorism Prevention Act Title III 2010 Annual Report, Office of the Director of National Intelligence, February 2011.
ultimately obtaining a security clearance. Responding to the number of jobs in Maryland that require some level of security clearance, the FMA has expanded Project SCOPE to include college students and existing members of the workforce.

Sparking interest in cyber careers

Speakers also noted that several incentive programs and outreach efforts by government agencies and private sector firms are proving to be effective ways of interesting children in STEM careers and should be given even greater public and private support in the future. These programs, speakers reasoned, could help generate essential cyber professionals in the future for government agencies, government contractors and other companies and organizations that play vital roles in the safety and prosperity of America.

Speaking at the FMA’s Cybersecurity Forum, Gudger pointed to federal financial incentives that are offered to students who pursue degrees in cyber. One incentive, which pays off student loans for cyber professionals, is already proving to be a success and ideally should be expanded.

Outreach programs to school children are triggering surprising effects.

George “Dennis” Bartko, Chief of the National Security Agency’s Cyber Task Force, explained how NSA’s program that sends agency mathematicians out to teach school children had a startling impact on his own household. Bartko’s son had come home from school one day suddenly excited about math. The boy explained that some people had come into his class and talked about code-breaking. Suddenly, mathematics was the key to doing something cool and exciting in his eyes. When Bartko asked his son who the people were, the boy said they were from the NSA.

“I said, ‘Do you know I work there too?’” Bartko recalled. “He said, ‘But Dad, these folks were really smart.’”

The Fort Meade Alliance is working to bolster students’ interest for STEM through two signature programs. Created in 2008, Tech Mania treats high school students to all-day events designed to give them hands-on exposure to cutting-edge technology developed in their own backyards. To date, more than 1,000 students have attended Tech Mania events. And the program appears to be having an impact. Four out of five students who attend a Tech Mania day, say the event increased their interest in technology and technology careers.

STEM Family Night exposes elementary school students, and their parents to hands-on demonstrations of local and leading technologies. The first STEM Family Night which was held at Arundel Mills in October 2010, also gave parents and children an opportunity to meet with public school officials from Anne Arundel and Howard counties to discuss their STEM programs. FMA has experienced increasing interest and participation at this single event from 600 students and parents in 2010 to more than 800 in 2011.

Professionals in the cyber industry have also suggested that school children should be made aware of the financial benefits of pursuing STEM careers. Careers in STEM fields tend to carry above-average salaries. Careers in cyber heighten salaries further due to the need for security clearances. Making students aware of those career and salary implications could create a greater incentive to pursue STEM and specifically, cyber careers.
Giesler, who regularly coordinates conferences for military and federal information workers, described the surprising results that came from inviting the First Robotics Team from Battleford High School, Va. to a conference luncheon. Giesler knew it would be a great opportunity for the students who had placed second in the national competition, to interact with accomplished technology professionals and maybe get ideas about future careers. What he hadn’t expected was that the interaction would trigger high-level IT discussions that would teach “the old timers” a few things.

“Those kids were wicked smart and those hardened military planners and folks who were back from Afghanistan or on their way [to Afghanistan] took to them like ducks to water,” Giesler said. “The reason was those kids had insights into a domain that a lot of the old timers simply didn’t. They were born into it. They operate in it on a daily basis. It was kind of interesting and magical seeing the older generation interacting with them. I was sitting at lunch discussing the challenges of migrating from IPV4 to IPV6 with a junior in high school.”

The cyber industry, speaker after speaker stressed, needs to keep increasing its commitment to programs that excite children about STEM fields if it is going to build a large and talented workforce to master cyber threats and opportunities in America.

Conclusion

Maryland is standing at the edge of an unprecedented opportunity — the opportunity to be the epicenter of America’s cyber industry. We have a critical mass of federal, cyber agencies in the state, and especially in the Fort Meade area. We have a high concentration of information technology companies and a highly educated workforce.

To take full advantage of that opportunity, however, Maryland must greatly increase both the quantity and quality of its cyber professionals.

- Critical thinking, analytical capabilities, leadership skills and strong communication skills are lacking in today’s new hires, even as these students graduate with core technology and engineering skills, forcing government agencies and companies to provide additional training internally for new hires.

- In order to provide thorough cybersecurity for the United States, it will be essential to create better avenues for building a workforce pipeline by generating interest in STEM/cybersecurity and by developing an effective security clearance process.

Individual companies have launched their own efforts to build that leading edge workforce. They have developed their own training courses, their own testing and certification procedures, even their own cyber universities. Private industry along with federal agencies have ramped up their outreach to grade school and college students in an effort to excite them about STEM studies and cyber careers.

To meet rapidly growing and changing demands for cyber experts, however, government agencies, private companies and the education sector will have to sustain even more vigorous efforts to excite, educate and graduate more American-born students in STEM fields.
Americans have already seen a myriad of examples of how that weapon can be used to damage a country. There are the 250,000 probes and scans that Department of Defense networks experience every hour. NASA’s Goddard Space Flight Center was attacked by a foreign power in an incident that delivered a wealth of classified information to another country.

However, the targets of cyber attacks don’t have to be limited to government sites in order to inflict real and dramatic damage on the security and prosperity of the nation. The private sector accounts for 80 percent of all cyber activity. Beyond the online operations of individual companies, entertainment sites, retailers and social networks, that activity stretches out to include the critical infrastructure of the nation — our power generation and distribution networks, our banking and finance systems, transportation networks, heavy industry and essential communications arrays.

Hackers have already attacked the Nasdaq and “we know all the major companies are being cyber hacked one way or another to get information,” said Congressman C.A. Dutch Ruppersberger, the ranking member on the House Intelligence Committee.

Imagine how much economic, physical and political damage cyber attackers could do if they successfully disrupted the PJM (Pennsylvania – New Jersey – Maryland) electrical grid, interfered with the New York Stock Exchange, meddled with the operations of the Calvert Cliffs nuclear power plant, disrupted air traffic control at Baltimore-Washington Thurgood Marshall International Airport, interrupted signaling on transportation networks, or disabled wireless communications networks that support everything from corporate teleconferences to 911 calls.

Air Force Maj. Gen. David N. Senty and Army Gen. Keith Alexander have both expressed concerns that future cyber attacks will be destructive, not just disruptive. “There is an awareness now ... about destructive tools that are out in the wild and those can do grievous damage to our physical infrastructure,” Senty said.1

Protecting such infrastructure is obviously vital to national security and well-being. At the Fort Meade Alliance’s Cybersecurity Forum, multiple speakers stressed that protecting America’s critical infrastructure will require strong public-private partnerships as well as a rigorous new approach to risk management in the private sector.

Breaking the barriers of imagination

As Director of Corporate Information Security for Constellation Energy Group, Michael Rossman believes he is squarely in the middle of the single most interesting private sector for cybersecurity. One of the largest energy companies in America, Constellation has more than 12,000 megawatts of generation capacity. It operates 55 plants including a “nuclear fleet” and, through Baltimore Gas and Electric Company, handles electrical transmission on a grid that stretches into 13 states. Its energy generation, management and supply operations serve Americans from coast to coast, including two-thirds of the companies on the Fortune 100 index. In downtown Baltimore, it also operates the largest commodities trading floor outside of New York City.

A successful cyber attack on Constellation could obviously do enormous damage. The Stuxnet virus made the prospect of an attack even more real.

Stuxnet, Rossman said, pushed cyber attacks on critical infrastructure out of the realm of the hypothetical and into the realm of the real and proven.

“Although we were amazed by Stuxnet, I think I could assemble a team of grad students — industrial engineers and software engineers — and repeat that,” he said. “I don’t think it was as such an incredible technological feat as it was a breaking of a barrier of imagination.”

Stuxnet, he said, showed that cyber attackers could reprogram industrial control systems to do things their designers never intended. It also showed that a cyber attack could be a multi-point attack, not just a single point of failure. That has changed industry’s thinking about the nature of cyber threats and the necessary response.

---

Constellation Energy has initiated multiple efforts to develop more robust and progressive cyber defenses, Rossman said. It has implemented new strategies to add cyber staff and train them in a variety of new skill sets, including designing cybersecurity systems and responding to incidents. It has also created a combined cyber and physical security organization that reports directly to Constellation’s management team. And it has pulled employees from disparate wings of the company together to work on cyber issues. Essentially, Constellation has embraced a new, broad-based, risk management approach to cyber.

“We need relationship- and team-building,” Rossman said. “In a business environment, cybersecurity risk is not merely having folks who have technical expertise. You need to build teams across different business units and groups. In critical infrastructure, I need to integrate teams of those who operate industrial control systems, who manage plants, who operate trading floors. And I need to obtain expertise in a team that allows us to understand what threats might exist against those assets.”

That broad-based approach to cyber defense, however, means that organizations like Constellation need to develop heightened problem-solving skills. Its employees need to be able to understand how business systems might be misused, imagine the possibilities for multi-point cyber attacks, and devise effective defenses against them.

Jeff Deason, a Senior Manager in the National Information Security Assurance group of the Federal Reserve, said that broad-based — and essential — approach to cybersecurity requires the operators of critical infrastructure to develop greatly expanded risk-management expertise. It also presents organizations with an additional challenge. Specifically, it triggers tough discussions about cybersecurity that involves everyone from newly graduated technicians to senior executives. Somehow, organizations need to harness all that disparate expertise and channel it into an effective cyber defense program that everyone can agree on it.

Private sector organizations, forum speakers suggested, need to instill cyber knowledge throughout many divisions and levels of their organizations from IT hardware technicians to risk-management executives and elsewhere. Companies also need to hire expert cyber auditors to verify that they are effectively and fully meeting their own cybersecurity plans and regulatory requirements.

Expanding public-private partnerships

Several speakers at the Cybersecurity Forum stressed that public-private partnerships will be essential to protecting America’s critical infrastructure — as well as its government — from cyber threats.
“What makes our country so unique is we have our government working in partnership with our contractors” on military, intelligence and homeland security issues, said Congressman Ruppersberger. “We will only make it as a country if we preserve this partnership.”

Col. George Lamont of the U.S. Air Force and Chief of Exercise and Training for U.S. Cyber Command proposed that systems and practices developed by U.S. Cyber Command should be shared with other federal agencies as well as the private sector. Public-private partnerships, he stressed, are essential to the success of cybersecurity developments and their effective utilization throughout American cyber space.

Jenny Menna, Director of Critical Infrastructure Cyber Protection and Awareness for the National Cybersecurity Division of the Department of Homeland Security (DHS), said the federal government has initiated several programs to expand its collaboration with the private sector on improving America’s cybersecurity.

- In September 2010, Cyber Storm III — part of DHS’s biennial exercise series that is the most extensive, government-sponsored, cybersecurity exercise — attracted record participation. That included eight cabinet-level departments, the White House, 11 states, 12 international partners and 60 private sector companies (a 50 percent increase from Cyber Storm II).
- The previous autumn, the federal government created the National Cybersecurity and Communications Integration Center to serve as a hub of national cybersecurity coordination.
- Also in 2010, the National Security Agency released Einstein 3, a pilot technology developed by NSA to automate the process of detecting cyber intrusions on civilian networks.

Such efforts, Menna said, will not only improve the effectiveness of cybersecurity in the public and private realm, but also reduce the considerable cost of developing cybersecurity systems in private enterprise.

More private enterprises need to look at cybersecurity as an overall enterprise risk-management issue that should be addressed at the board level not simply at the level of an IT department, Menna said. The business community, she added, can greatly improve the country’s overall cybersecurity by being vigilant, truly understanding its network and traffic, developing risk-management and incident-response plans, carefully monitoring all cyber activity, and collaborating with government.

Confronting a new scientific challenge

Government, in turn, could do tremendous things to help excite the American workforce about cyber opportunities and thereby help the private sector tap vital and scarce expertise, several speakers said.

Howard Clifford, a Hewlett Packard Distinguished Technologist and the company’s Chief Technologist for the U.S. Intelligence Community focusing on cybersecurity, argued that government needs to address the painfully evident shortage of American scientists, mathematicians, engineers and technologists.

“What motivated other cultures to learn math, learn the sciences, and follow this path?” Clifford asked.

The country needs more homegrown cyber experts in hard sciences, engineering and information technology, but also in a broad spectrum of professions from medicine to entertainment. Government, he argued, has the power to motivate a generation to embrace and prepare for careers in cyber just as it motivated a generation to study mathematics, engineering and the hard sciences in order to explore space.

In May 1961, President John F. Kennedy announced before a special joint session of Congress his ambitious goal of winning the space race. “I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the Earth. No single space project in this period will be more impressive to mankind, or more important for the long-range exploration of space; and none will be so difficult or expensive to accomplish.” The President called on “every scientist, every engineer, every serviceman, every technician, contractor, and civil servant to give his personal pledge that this nation will move forward, with the full speed of freedom, in the exciting adventure of space.”

The task was daunting and borne out of fear that the Soviets would dominate space and further threaten America, Clifford said. Yet that initiative prompted huge numbers of children to embrace a vision and get excited about an enormous, ambitious, scientific challenge. As a result, in the 1960s and 1970s America graduated elevated numbers of mathematicians, scientists, engineers and PhDs.

Now, “we’ve got to make cyber cool,” Clifford said. “We’ve got to put it in terms and language that kids understand so that they will respond. We have to make it into something that really motivates them.”

Conclusion

Although most Americans are blissfully unaware of the threat, cyber attacks and misdeeds could cripple infrastructure that is critical to our lives, including the banking system, telecommunications, energy grids, air traffic control and first responders’ systems. Some cyber experts warn that such an attack is inevitable. Protecting the nation’s critical systems will take strong partnerships between government agencies and private companies.

The FMA’s Cybersecurity Forum raised key points about the pervasive threat:

- A threat of cybersecurity breaches exists in every industry and has the potential to affect every U.S. citizen;
- Every person — at home, at work and in the community — must be vigilant and participate in good cybersecurity hygiene; and
- Cybersecurity risk management will require strong partnerships among all government agencies, corporate industries and private citizens to be successful and insure the safety of the United States.

Some American corporations are already embracing a new approach to cyber risk management — one that brings senior management, technology experts and employees from all facets of a company together to imagine potential risks and create both defensive and recovery plans.

However, efforts to protect America’s critical infrastructure are challenged by the same overarching problem that faces government agencies and cybersecurity companies, a shortage of skilled workers. At the Cybersecurity forum, speakers suggested that America needs a “sputnik moment” in cyber — a development that inspires the nation to study science, engineering and mathematics, to develop new technologies and to excel as a nation in cyber space.
Training the Cyber Warrior
Lack of STEM students and cyber training programs challenge industry

“Often when people talk about cyber space, they come right down to the technical aspect of the space. We realize that it is a space or a domain that is starting to become something like the land, the sea, the air or space. The skills needed are not just the skills to create it, maintain it, modify or enhance it. There are now so many other disciplines needed. I think it is hard to think of any disciplines that don’t work into that domain.”

~ George “Dennis” Bartko, Cyber Task Force Chief, National Security Agency

Finding, exciting, training and retaining a vast, diverse cyber workforce is, without doubt, the consuming challenge facing government agencies and private companies active in the cybersecurity field. Science, technology, engineering and math (STEM) classes aren't captivating enough American grade school children and university STEM programs aren’t churning out enough American-born graduates. Existing technology workers need additional training to become proficient in cyber. Government agencies, academic institutions and private companies still need to identify essential cyber skills and devise core curriculum and certification programs.

And the needs don’t end there.

Although discussions about the cyber workforce typically fixate on the need for engineers and IT professionals, the industry as a whole can only function properly if it has a well-connected system of engineers, IT professionals, scientists, linguists, intelligence agents plus experts in the fields of finance, transportation, communications, healthcare, heavy industry, electricity grids, policy making, international diplomacy and many others.

The single most repeated message at the Fort Meade Alliance’s Cybersecurity Forum was that all facets of the cyber industry need to work together, more vigorously and more tactically to create the cyber workforce America needs.

A national shortage of STEM students

Deborah Bonanni, Chief of Staff for the National Security Agency, describes the lack of American children pursuing STEM studies as nothing less than a “national education crisis.”

Freeman Hrabowski, President of the University of Maryland Baltimore County (UMBC), said Americans’ attitudes toward science are discouraging children from pursuing STEM studies.

“We in America have accepted that science is just not for everybody. We send messages to students all the time that, ‘This is not really for you,’” Hrabowski said. “One of the reasons American (students) aren’t more excited about science is that adults themselves aren’t excited. Most (students have been weeded out before they even get to college.”

Hrabowski dismisses suggestions that some students aren’t smart enough to study science or math, insisting instead that “Your teacher wasn’t innovative enough.”

Science and Engineering Undergrads
Although minority involvement in STEM fields of study is slowly rising, Hispanics, African Americans and other minorities are still underrepresented in those fields.

![Undergraduate Enrollment in Science and Engineering in American Colleges](image)

Source: National Science Foundation
Universities, he argues, need to change the atmosphere of STEM programs from a highly competitive situation to a highly supportive situation.

At UMBC, he said, “we say, ‘If we accept you in science, you have the ability to do it, and we’ll help you succeed.’ What has made the difference at UMBC is the way we encourage group work and teachers to rethink their approach to the classroom. The results are significantly more students are succeeding.”

A March 2010 eSecurity Planet article entitled “U.S. Faces Cybersecurity Gap without Training, Education” explored the consequences of that crisis: “Working in concert with the government, the private sector has made significant strides in improving software security and ferreting out vulnerabilities in the supply chain, but the flow of cybersecurity experts graduating from the nation’s universities with advanced degrees remains anemic, according to Richard Marshall, Director of Global Cybersecurity Management at the Department of Homeland Security.”

An ACT report entitled “The Condition of College and Career Readiness: Class of 2010” illustrates how the interests of Maryland students do not meet the growing need for cyber professionals. According to the report, more Maryland students express plans to major in health sciences, education, and sales/marketing than in computer or information specialties. The ACT analysis projected a 15 percent increase in job openings for professionals in computer/information specialties but just 3 percent growth in the number of Maryland students entering those fields of study.

The analysis also indicated that Maryland’s high school graduates would not be entirely prepared to enter such high-growth technology fields even if they opted to. ACT assessed the college readiness of 2010 graduates. Among those who expressed interest in computer/information careers, 63 percent met English benchmarks for college readiness, 48 percent met reading benchmarks, 49 percent met mathematics benchmarks and just 32 percent met science benchmarks.

The report showed that many Maryland high school graduates are not prepared to enter STEM fields generally. Just 53 percent of graduates scored high enough to be considered ready to tackle college mathematics and just 37 percent were ready to take college science courses. The report also showed large disparities in college-readiness among different groups of students.

The report’s analysis of Grade 10 students concluded that overall they would be somewhat more college-ready. ACT stressed that solid education in elementary and middle school is vital to helping children get ready to tackle college and careers. “The level of academic achievement that students attain by eighth grade has a larger impact on their college and career readiness by the time they graduate from high school than anything that happens academically in high school,” the report stated.

Cyber Maryland noted that the State, as well as many individual school boards, has initiated programs to bolster STEM programs and attract more students. Governor Martin O’Malley created the STEM Task Force of the P-20 Leadership Council to draft recommendations to better prepare Maryland students for careers in a STEM-based economy. Anne Arundel County Public Schools now offers a suite of STEM programs for pre-K to Grade 12 students throughout the academic year and the summer break in order to engage students in challenging STEM projects. Baltimore County Public Schools has partnered with The Johns Hopkins University Center for Technology in Education and JHU’s Applied Physics Laboratory to

create a prototype Virtual Learning Environment that uses game-like experiences to augment existing math and science curricula.¹

At the University of Maryland, educators are reaching out to high schools in an effort to make students more ready to tackle university-level engineering classes. Leigh Abts, an associate professor of engineering and education, said many high school graduates aren’t ready to tackle the rigors of calculus when they reach university and often lack the problem-solving skills to adapt to the demand of engineering courses. Consequently, educators have developed an Advanced Placement class in Engineering Math to both build math skills and to show students how calculus and other demanding math courses will relate to the core work of an engineer.

The University of Maryland has also developed an AP course in Engineering Design. The course is designed to address two education issues. First, many students have little exposure to actual engineering projects in high school — a situation that noticeably impairs their ability to succeed in engineering school, Abts said. Second, the current high school education system which compels students to deliver the one right answer to any question, does not foster creative, problem-solving skills and it often leaves students floundering when they face an open-ended problem like the challenges regularly presented to engineers. The AP Engineering Design Program, Abts said, exposes students to the work and challenges of an engineer, and requires them to solve open-ended problems in order to develop workable solutions.

Abts hopes the programs will both improve students’ college readiness and also ease the disturbingly high dropout rates seen at some engineering schools around the country. While the University of Maryland College Park boasts a relatively high retention rate of 70 percent in its engineering school, many engineering schools and other STEM programs see large numbers of students switch majors or leave the university without ever finishing their STEM degrees.

Through an extensive study, the Higher Education Research Institute of the University of California, Los Angeles found that STEM programs across the nation suffer ‘alarmingly’ high dropout rates. Just one-third of white students and 42 percent of Asian-American students who started college as STEM majors, graduated with STEM degrees within five years. Among some minorities, the degree-completion rates were even worse. Just 22.1 percent of Latino students, 18.4 percent of black students and 18.8 percent of Native American students completed their STEM degrees.

At the same time, students who entered non-STEM degree programs posted considerably better rates of completing their degrees within four years: 61.3 percent among white students, 65 percent among Asian-Americans, 56.1 percent among Latino students, and 49 percent of black students.²

The Fort Meade Alliance vigorously supports efforts to improve STEM education in Maryland. The FMA has worked to created Tech Mania Days, STEM Family Nights and the Homeland Security Signature Program at Meade High School, and plans to continue partnering

---

with education officials to grow this vital portion of Maryland schools, colleges and universities.

**Concerns about quality programs and foreign students**

Leaders in the cyber industry stress that the state – and the entire country – needs to work diligently to both increase the quantity of STEM students while also increasing the quality of college graduates and cyber professionals.

In the February 2011 edition of The Armed Forces Journal, Lt. Col. David M. Hollis and Katherine Hollis wrote, “A critical shortage of cyberspace-domain-trained and certified personnel affects the U.S. quantitatively and goes beyond mere education requirements. There is potentially an even greater shortfall in cyberspace workforce in the event of a major event in cyberspace. Cyberspace-domain assets and resources are not adequately trained or organized to meet the potential threats. The national education system needs to be overhauled and reformed to produce an effective number of qualified personnel for both government and private sector cyberspace-domain requirements.”

A recent cyber competition sponsored by the National Security Agency and software developer Top Coder seemed to verify Paller’s assessment. Programmers from China and Russia dominated every competition category from writing algorithms to designing components. From a field of 42,000 competitors, 70 people advanced to the finals. Among them, 20 were from China, 10 from Russia and only two from the United States.

The United States has ranked 20th of 24 countries for the percentage of college graduates whose first degree was in science or mathematics. In 2009, Congressman C.A. Dutch Ruppersberger said, China graduated seven times more STEM students and rocket scientists than the U.S. and many of those American graduates were actually foreign students.

Several speakers at the Fort Meade Alliance forum noted that America is grappling with one added wrinkle in generating STEM professionals, namely many students in STEM programs at American universities are foreign nationals.

---

Recent findings from Compete America, the Alliance for a Competitive Workforce, indicate that nearly half of all Master’s Degrees (42 percent) in engineering awarded by American universities and more than half of all PhDs (53 percent) in engineering went to foreign students. The highest percentages of foreign-born graduates actually came from the University of Maryland where 171 of 373 Master’s Degrees in engineering (46 percent) and 83 of 144 PhDs in engineering (58 percent) went to foreign students.¹

Taking a closer look at the United States, almost every state has at least 20 percent of Master’s degrees and more than 50 percent of PhDs in advanced engineering awarded to foreign nationals. In Maryland, 23 percent of Master’s degrees and 53 percent of PhDs are awarded to foreign nationals.²

Unlike in previous decades, many of those foreign students do not remain and work in the United States after graduation due to anti-immigrant sentiments and heightened incentives from China and other countries for STEM graduates. Even if they did stay in America, those graduates would not be able to take core cybersecurity jobs because they would not be able to qualify for federal security clearances.

¹ “Stop the diploma drain,” Compete America, 2010.
² “Engineering & Technology Degrees 2010,” America Association of Engineering Societies

### U.S. Engineering Advanced Degrees Awarded to Foreign Nationals by State (2009-2010 academic year)

<table>
<thead>
<tr>
<th>State</th>
<th>Masters</th>
<th>PhDs</th>
<th>State</th>
<th>Masters</th>
<th>PhDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>35%</td>
<td>24%</td>
<td>Montana</td>
<td>32%</td>
<td>N/A</td>
</tr>
<tr>
<td>Alaska</td>
<td>24%</td>
<td>67%</td>
<td>Nebraska</td>
<td>2%</td>
<td>15%</td>
</tr>
<tr>
<td>Arizona</td>
<td>62%</td>
<td>62%</td>
<td>Nevada</td>
<td>48%</td>
<td>67%</td>
</tr>
<tr>
<td>Arkansas</td>
<td>14%</td>
<td>89%</td>
<td>New Hampshire</td>
<td>32%</td>
<td>20%</td>
</tr>
<tr>
<td>California</td>
<td>42%</td>
<td>48%</td>
<td>New Jersey</td>
<td>48%</td>
<td>61%</td>
</tr>
<tr>
<td>Colorado</td>
<td>20%</td>
<td>30%</td>
<td>New Mexico</td>
<td>39%</td>
<td>49%</td>
</tr>
<tr>
<td>Connecticut</td>
<td>73%</td>
<td>20%</td>
<td>New York</td>
<td>56%</td>
<td>65%</td>
</tr>
<tr>
<td>DC</td>
<td>29%</td>
<td>41%</td>
<td>North Carolina</td>
<td>57%</td>
<td>53%</td>
</tr>
<tr>
<td>Delaware</td>
<td>N/A</td>
<td>N/A</td>
<td>North Dakota</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Florida</td>
<td>45%</td>
<td>59%</td>
<td>Ohio</td>
<td>46%</td>
<td>65%</td>
</tr>
<tr>
<td>Georgia</td>
<td>48%</td>
<td>54%</td>
<td>Oklahoma</td>
<td>57%</td>
<td>74%</td>
</tr>
<tr>
<td>Hawaii</td>
<td>18%</td>
<td>82%</td>
<td>Oregon</td>
<td>35%</td>
<td>15%</td>
</tr>
<tr>
<td>Idaho</td>
<td>12%</td>
<td>4%</td>
<td>Pennsylvania</td>
<td>37%</td>
<td>60%</td>
</tr>
<tr>
<td>Illinois</td>
<td>56%</td>
<td>59%</td>
<td>Rhode Island</td>
<td>21%</td>
<td>63%</td>
</tr>
<tr>
<td>Indiana</td>
<td>42%</td>
<td>58%</td>
<td>South Carolina</td>
<td>51%</td>
<td>55%</td>
</tr>
<tr>
<td>Iowa</td>
<td>33%</td>
<td>61%</td>
<td>South Dakota</td>
<td>45%</td>
<td>25%</td>
</tr>
<tr>
<td>Kansas</td>
<td>42%</td>
<td>62%</td>
<td>Tennessee</td>
<td>22%</td>
<td>48%</td>
</tr>
<tr>
<td>Kentucky</td>
<td>29%</td>
<td>76%</td>
<td>Texas</td>
<td>52%</td>
<td>54%</td>
</tr>
<tr>
<td>Louisiana</td>
<td>75%</td>
<td>60%</td>
<td>Utah</td>
<td>23%</td>
<td>44%</td>
</tr>
<tr>
<td>Maine</td>
<td>19%</td>
<td>38%</td>
<td>Vermont</td>
<td>28%</td>
<td>27%</td>
</tr>
<tr>
<td>Maryland</td>
<td>23%</td>
<td>53%</td>
<td>Virginia</td>
<td>32%</td>
<td>52%</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>40%</td>
<td>47%</td>
<td>Washington</td>
<td>19%</td>
<td>44%</td>
</tr>
<tr>
<td>Michigan</td>
<td>46%</td>
<td>56%</td>
<td>West Virginia</td>
<td>35%</td>
<td>72%</td>
</tr>
<tr>
<td>Minnesota</td>
<td>25%</td>
<td>63%</td>
<td>Wisconsin</td>
<td>34%</td>
<td>50%</td>
</tr>
<tr>
<td>Mississippi</td>
<td>41%</td>
<td>55%</td>
<td>Wyoming</td>
<td>38%</td>
<td>64%</td>
</tr>
<tr>
<td>Missouri</td>
<td>31%</td>
<td>54%</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: “Engineering & Technology Degrees 2010,” America Association of Engineering Societies
**Patriot Hackers**  
**Cyber Experts Find Talent in Unconventional Places**

What if some of the most talented, young operators in cyberspace were nowhere near a college classroom and unlikely to ever show up on a recruiter’s radar?

Executives in the cybersecurity industry say talent in this emerging and rapidly changing field can come from places far beyond the high-tech mainstream.

Speaking to the Air Force Association CyberFutures Conference at National Harbor, Md. in 2011, Lynn Dugle, president of Raytheon Corporation’s intelligence information systems businesses, described how her company typically focuses its search for new cyber professionals on prestigious universities and students with impressive grade point averages. Yet that process hasn’t always been the best path to a great hire. National Defense magazine summarized Dugle’s explanation:

None of Raytheon’s recent and most impressive hires have come from the campus culture. One had only a GED and was working in a pharmaceutical plant stuffing pills into bottles. In the evenings, he outshined the rest during online hacker competitions.

“That person would have not gotten through the normal Raytheon recruiting process,” Dugle said.

The situation was similar for another recent hire who the company found single-handedly defeating groups of hackers in a team competition. He was a teenager, still in high school, when Raytheon took notice.

The same article stressed that cybersecurity companies and agencies can benefit by expanding their recruiting efforts beyond college campuses: “Academic programs alone won’t attract the most promising talents to the field... In the past 30 years, the most innovative cyber operators seen have been military kids with no more than a high school education.”

Cyberspace Education and Training, a report by the National Security Cyberspace Institute, notes that federal agencies and private companies have begun hosting cyber competitions and camps to find talented, young cyber operators. The U.S. Cyber Challenge — three competitions sponsored by the Department of Defense, the Air Force Association and the SANS Institute — challenge high school students and others to penetrate cyber defenses and find solutions to digital forensics problems that currently can’t be solved. “These competitions and camps are designed to identify 10,000 young Americans with the interest and computer skills to become the next generation of cybersecurity professionals,” the report states.

In the Armed Forces Journal in February 2011, Lt. Col. David M. Hollis and Katherine Hollis described the radically different approach that the Chinese and Russian governments have taken to recruiting and training cyber workforces.

They and the Russians often use their “patriot hacker” community to conduct much of their cyberspace mission.

“Every military district of the People’s Liberation Army runs a competition every spring, and they search for kids who have gotten caught hacking,” said [Alan] Paller [of the SANS Institute]. One of the Chinese youths who won that competition had earlier been caught hacking into a Japanese computer, Paller said, only to be rewarded with extra training. “Later that year, we found him hacking into the Pentagon,” Paller said. “So they find them, they train them, and they get them into operation very, very fast.”

Inspiring a generation

This national shortage of STEM students and future cyber experts presents educators and the cyber industry with multiple challenges. The first is the vital need to get more children excited about STEM education and related careers.

The NSA has created several initiatives to “excite kids” about STEM, cyber and other prospects in the security and intelligence fields, Bonanni said.

“Our mathematicians take it on as a personal crusade to make sure that they are reaching out in the K-12 arena to make sure the math teachers are provided with some new, creative ways of creating curriculum,” Bonanni said, adding that NSA mathematicians also mentor students and do presentations to numerous math classes.

In addition, the NSA — where women fill 40 percent of leadership positions — is making special efforts to connect with young, university women, inform them about career options in the computer science field and

---

encourage them to pursue PhDs in the field. Senior NSA staff members have hosted a session for university women in STEM programs — many of whom were teetering on whether to stay in those fields — to discuss career opportunities in STEM. Currently, American women as well as African Americans and Hispanics account for disproportionately low percentages of STEM students and professionals.

Bonanni said she would like to see NSA expand its outreach efforts to spread across the state and country, and branch into STEM disciplines other than mathematics.

“The math community at NSA has led the way in outreach to turn on kids to majoring in math and I think we could do more in the area of computer science and other sciences,” Bonanni said. “We’ve got to turn this young generation onto science and onto these STEM disciplines. It’s about this next generation and whether or not we can show them the innovation, the creativity, the power that resides in the scientific disciplines. Once we get them educated in this area, there is no end to the cool jobs.”

Multiple industry experts have stressed the need for additional efforts — including educational partnerships, outreach programs, internships and scholarships — by government agencies and private companies to excite and inform America’s youth about STEM education and cybersecurity careers.

Richard Marshall, Director of Global Cybersecurity Management at the Department of Homeland Security, has appealed for both federal and private investment in higher education programs that could provide tuition assistance to draw students into cybersecurity programs, noting that free education is a powerful lure.

“Look at all the great football and basketball programs,” Marshall said. “They’re all on scholarships. They’re not playing for fun — they’re playing for money. We need to do the same thing with our computer science students.”

George “Dennis” Bartko, Chief of the NSA’s Cyber Task Force, is a vocal supporter of internship and work study programs for students. Bartko admitted that he didn’t even know what the NSA was until he began working with the agency in a co-op work term during his sophomore year.

NSA offers on-the-job training opportunities for students through work/study programs. The programs are designed for high school students who are enrolled in either business computing or office technology classes. Participants are hired on a part-time basis and work either as an office assistant or computer aide, operating sophisticated equipment. Participants then have an opportunity to be hired as an intern or a permanent staff member. The agency which does considerable outreach to schools and universities, is now aiming to generate 10 percent of its new staff annually from its pool of graduating interns.

“A large part of the (skilled cyber worker) shortage problem is education. While several programs at colleges teach the basics of cybersecurity, there are few that can be considered state of the art.”

- Dickie George, NSA Information Assurance Technical Director

The Defense Information Systems Agency is also heavily leveraging its internship and part-time student worker programs, said Mark Orndorff, Director of DISA’s Program Executive Office for Information Assurance and NetOps. The programs, he noted, give students exposure and experience in the field while also preparing them to obtain security clearances. DISA which is also striving to select 10 percent of its new employees from each year’s graduating interns, gets one other advantage from the student work programs, Orndorff said. Interns regularly give training sessions on new technologies to DISA executives.

Some cybersecurity experts say vigorous public-private partnerships could greatly advance efforts to get more students excited about STEM and cyber, and also improve the quality of STEM education in Maryland schools. Such partnerships could enable top subject matter experts (SMEs) to go into classrooms, give presentations, work with students on projects and inspire more young people. The SMEs could also work with teachers on enhancing curriculum, help tap additional resources, and provide internships, work terms and other opportunities to existing teachers or education students so that they could get real-world experience in the STEM and cyber fields.

Developing a new cyber curriculum
A second challenge facing industry leaders and educators who want to generate future cyber warriors, is defining, developing and delivering the necessary training.

The relatively young cyber industry is still trying to gain a thorough understanding of the skill sets that will be needed in the cyber workforce. As previously discussed, the industry doesn’t yet have a complete list of cyber certification requirements nor the curriculum standards and courses needed to reach those requirements.

Cyber Maryland states that cybersecurity includes an extensive set of discrete technologies, capabilities and services stemming from the computer information and network security fields. Most colleges and universities, however, are not yet set up to foster that “considerable set” of cyber skills. Those gaps in curriculum have left many organizations in the cyber industry wrestling with the fact that they must provide additional training to new hires in order to make them proficient in the cybersecurity field.¹

According to Dickie George, Information Assurance Technical Director of the National Security Agency, “A large part of the (skilled cyber worker) shortage problem is education. While several programs at colleges teach the basics of cybersecurity, there are few that can be considered state of the art.”

Jim Lewis, Director of Technology and Public Policy Programs at CSIS, says the “broader problem is deeply rooted in education, with academic programs that don’t produce the kind of cyber people we need.”

Meeting that training need will require educators to deliver programs on core technologies and much more. It may also mean that students who are earning education degrees and intend to teach STEM courses, should complete coop terms within STEM fields before graduating.

Given that the cyber industry is evolving so quickly, mastery of numerous computer hardware and software products is core to the cyber warrior, said Joseph Pacileo, Vice President of Cyber Operations at ManTech. “These are the bottom line skills that are absolutely critical to our future.”

And that training cannot cease on graduation day. Industry experts at the FMA Cybersecurity Forum stressed the need for existing workers to continuously update and expand their skills. Computer scientists must realize that their training must be continually updated to cover emerging technologies and extreme situations.

“We’ve got to turn this young generation onto science and onto these STEM disciplines ... Once we get them educated in this area, there is no end to the cool jobs.”

- Deborah Bonanni, National Security Agency

Speakers also stressed that top-notch technical training must be augmented with training in vital “amorphous skills,” including communication, leadership, problem-solving, and analytical and creative thinking.

Finally, cyber training must spread well beyond technical fields in order to build a complete, expert cyber workforce. Professionals in business, healthcare, communications, energy, public policy and countless other fields will need cyber training in order fully defend the country.

Robert Giesler, Vice President for Cyber Programs at SAIC, described a three-year stint he served in the Office of the Secretary of Defense. The early days of cybersecurity were complicated by the lack of public policy experts who understood any technical aspects of cyber, he said. Technical experts from NSA would come into Washington and deliver technical briefings on cyber only to be met with glazed faces of public policy officials.

America needs to begin cultivating cyber diplomats, cyber policy-makers and other cyber professionals whose expertise stretches far beyond the technical. The next generation of cyber professionals, he concluded, will need to be multi-disciplinary with skills in technology, intelligence, public policy and many other fields.

Conclusion
It’s been called a “national crisis in education.” The shortage of American students engaged in STEM studies is seen in test scores that show many high school graduates are unprepared to face college courses in mathematics and science. It is seen in the low numbers

of students entering STEM degree programs in university and in the high numbers of advanced STEM degrees that American universities award to foreign nationals.

That shortage has widespread ramifications for America’s ability to remain competitive and secure in an evolving global economy. One sector which is acutely affected, is cybersecurity.

America is not only generating too few STEM graduates, but those graduates are often inadequately trained to assume the daunting and fast-changing responsibilities of cyber professionals due to gaps in curriculum and the lack of certification standards. In addition, cyber expertise needs to expand beyond the ranks of IT professionals and engineers to include policy makers, business managers, energy executives, financiers and numerous other professionals.

Federal agencies and private companies involved in cybersecurity as well as the State of Maryland, local colleges and school systems are making admirable efforts to address the STEM crisis. Fully resolving this shortage, however, will require added vigor by all parties to bolster STEM programs, find ways to excite students about the field, clearly identify needed cyber skills, establish certification standards, and ensure that American universities and colleges graduate ample numbers of American-born students from advanced STEM programs.

It is evident that:
• Early academic achievement has a larger impact on college and career readiness than high school years. Consequently, programs to advance STEM education must target younger students.
• The country faces a severe crisis in the number of college undergraduate and graduate students who can qualify for security clearances, and needs to look at lessening the number of foreign students enrolled in STEM programs at U.S. colleges and universities.
• Just as NASA developed space engineers by highlighting the “race to the moon,” the pursuit of cybersecurity needs to be highlighted.
• Education, at all levels, needs to be enhanced to include the complex skill sets and diverse facets of professional training required in the cybersecurity warrior. Our educational institutions need to supply the industry with well-trained workers who are prepared to begin work without needing remedial training within corporations or federal agencies.
1. There are very serious concerns about the number of foreign students in U.S. colleges and universities, which prevents producing a quality workforce able to fill the pipeline and qualify for security clearances.

Issues surrounding security clearances continue to demand attention. The need to create a “pipeline” of cleared workers continues to be one of the very critical factors in making Maryland a cybersecurity hub. While the process has improved, the private industry support to federal government contracts continues to struggle to hire skilled, qualified and security clearance eligible employees to meet contract requirements and schedule deadlines.

The greatest obstacle remains the influx of foreign students in STEM disciplines in college 4-year and graduate programs, occupying slots, which could be awarded to students with U.S. citizenship. With Maryland awarding 53 percent of engineering PhDs to foreign students who not only cannot qualify for a security clearance, but in many cases go back to use newly learned skills in their country, the FMA is very concerned for our future workforce.

2. The CyberSecurity industry workforce shortage is critical and, in many cases, this is exacerbated by the need for the Industry to provide additional on-the-job training for new hires, even in the case of many newly hired graduates with Master’s degrees.

A concern was expressed for new hires involving the lack of professional “soft” skills necessary for employees to become effective cyber warriors. These warriors are required to effectively share intellect within the organization, using strong communication and leadership skills. They receive additional training after hiring in the mission domain, orientation with mission standards tools and techniques, engineering and technology knowledge and the integration of critical thinking, analytical capabilities, risk management and innovation to be effective.

These skills are difficult to quantify for education and present a challenge being incorporated into standard curriculums. However, as an example, while Information Assurance skills or certification provides a technology skill, these skills alone in the cybersecurity industry do not qualify the employee to be “work-ready.” Without understanding the mission domain, standards, tools, technology, risk management, communicating the concept, using innovative thoughts to integrate other technology skills into solving the problem or having the ability to analyze and quantify the problem to outline the threats and outcomes, there is an “incomplete” cyber warrior who is not “work-ready.”

3. There is a critical need for partnerships between government, industry, educators and the community.

Partnerships are viewed as important enough that government has indicated willingness to rotate industry personnel into agencies to continually bring fresh concepts and new critical thinking to the issues facing our cyber world. The private sector, which requires cybersecurity in every type of industry, is faced with continually reaching out for additional training, or through contracted services, so their corporate intellectual capital, products and services remains free from invasion or theft. This partnership would also need to highlight a concern discussed by every panelist for in-house training and adherence to online security measures. The panelists feel one of the greatest threats to any organization is the insider threat from employees invading systems, either purposefully or in error. Cybersecurity “hygiene” will be an essential part of every user’s online training.

4. Deborah Bonanni, in her keynote address at the FMA Cybersecurity Forum, stated that “the lack of American children pursuing STEM is nothing less than a national crisis.”

While this is the last of the key points being discussed, the Fort Meade Alliance feels strongly this is one of the most importance. None of the key points discussed in this white paper will be able to be implemented without changing the current model for student involvement in STEM career interests. An analogy has been used in various articles about the development of the “Race to the Moon” concept used by NASA engineers years ago to encourage interest in the space sciences. This same type of dedicated focus on the development of a STEM “Race into CyberSpace” must be developed to give the United States an opportunity to be successful in this field.

Early involvement is key to creating the pipeline for STEM interest and every industry, regardless of the products or services offered. All private companies as well as the public-sector government agencies require cybersecurity warriors to insure protection of intellectual capital, products, services, and the security of our Nation. This early focus should provide effective results because the early integration will allow skills to be brought into teaching throughout the student’s school years, rather than trying to impose an “overload” of training in their higher education and workforce development.

Early involvement would also address the need to increase the number of students that are U.S. citizens in STEM disciplines, which could support more U.S. citizen STEM students in our colleges and universities. This would create a greater pipeline of potential workers able to fill cybersecurity positions in the U.S. government and companies providing support to U.S. government agencies, especially those requiring security clearances.
Expansions of federal facilities involved in cyber, innovations by high-tech companies and smart partnering between public and private sectors are creating unique and enormous opportunities for Maryland to be the epicenter of America's cybersecurity. Key to this success is the ability to deliver a qualified workforce.

Maryland is already home to unparalleled federal cyber assets. The Fort Meade region serves as headquarters for the National Security Agency, U.S. Cyber Command, the Defense Information Systems Agency and the cyber commands for the U.S. Navy and Marine Corps. The greater Washington area now surpasses Silicon Valley and New York City in total number of cyber jobs.

Securing a leading role in America's cybersecurity industry, will not come easily. In this extremely competitive and rapidly changing industry, Maryland needs to continue to bolster our education system in science, technology, education and mathematics (STEM) and sustain strong public-private partnerships to create the workforce and business environment needed to grow and sustain our ability to address cyber needs.

America isn't generating enough college graduates in computer science, engineering, mathematics and the hard sciences to meet growing needs for highly skilled, critical thinkers in the cyber domain who are eligible for security clearances. Many Maryland graduates in those sought-after STEM fields are foreign nationals and consequently ineligible for jobs in the U.S. federally-focused cyber public-private sectors. We need to work together to create ever improving STEM programs, motivate more students to focus on STEM fields and graduate more U.S. citizens from Maryland colleges/universities to fill critical cyber needs.

Maryland schools, colleges and community groups are stepping up efforts to attract students in STEM programs. The Fort Meade Alliance (FMA) has hosted Tech Mania Days and STEM Family Nights over the last four years to showcase technology applications, demonstrate how innovations coming out of Maryland companies can solve real world problems, and fuel students' interest in STEM-based careers. The FMA created Project SCOPE training that teaches middle and high school, college/university students and workforce development organizations about the nature, requirements of obtaining security clearances. The February 2011 FMA Cyber Education Forum was unprecedented in bringing leaders from federal cyber agencies, cyber companies, academic institutions and elected officials together to probe the overall requirements for cyber workforce, training needs and how public/private sectors need to work together to develop and sustain this workforce.

Maryland's elected leaders are actively pursuing cyber. Gov. Martin O'Malley created two public-private partnerships — the Governor's Cyber Workforce Investment Board and the Cybersecurity Commission — to bring public/private sector experts, heightened workforce development, vital infrastructure and business-friendly policies. Sen. Barbara Mikulski has drafted legislation that would triple federal scholarship funding for students striving to enter the federal cyber workforce and create a National Cyber Center of Excellence at NIST in Maryland for public and private experts to forge partnerships, advance technologies and create cyber jobs.

Maryland has all the components needed to be the epicenter of America's cybersecurity. To lead this challenging industry, we need to tackle the issues of education and workforce development, and continue to build vigorous public-private partnerships. By growing our expertise, we will not only lead cyber, but we will also gain the satisfaction of knowing that our work is protecting our nation.
Booz Allen Hamilton, a leading strategy and technology consulting firm, has deep experience and expertise working with clients to develop a cyber-ready workforce and associated leadership. Cyber threats are constantly evolving, becoming more complex and happen at network speed. In order to meet the challenge of cyber issues, the knowledge and skills of the cyber workforce must be just as deep, dynamic and ready to respond.

Workforce readiness does not happen by accident. Organizations must invest in acquiring the right talent to support cyber operations. They must start now to develop the highly trained and qualified cyber workers, managers, and leaders who will be critical to protecting the organizations from today’s threats and from those that emerge in the next 5, 10, and 20 years.

To help address the technical skills for cyber analysts Booz Allen has created a Cyber University, to increase the firm’s talent pool to support government agencies and a varied client set. The Cyber University conducts boot camps, advanced vendor training and mentoring programs, and technical certifications where our cyber professionals can acquire new competencies while having the flexibility to work full time.

In addition, the firm makes a point to stay abreast of the latest technologies. We provide analytical and technical training for the intelligence and defense communities, and we have extensive expertise in analytical skills, tools, techniques and procedures. Coupled with our Cyber University, Booz Allen is able to provide the necessary expertise and help our clients develop a workforce that is cyber ready, no matter what the threat.

Booz Allen has a strategic partnership with University of Maryland University College (UMUC) to offer students online graduate certificates in cybersecurity. The program, which blends Booz Allen’s knowledge of emerging cybersecurity needs with UMUC’s reputation of excellence, comes as the U.S. strives to build a competitive, forward-thinking cyber workforce.

The courses are available today to Booz Allen employees who are graduate-level students interested in taking advantage of the Web-based initiative to enhance their knowledge of the expanding role of cybersecurity. They became available to the general public in the spring 2011 semester. The company’s tuition reimbursement program assists in funding Booz Allen staff enrollment. We have learned that government agencies and businesses need to think beyond traditional, prescribed processes to recruit their cyber talent. Sourcing and recruiting practices need to be viewed as a marketing and outreach program, not just a job posting to a web site. Recruiters need to think beyond hiring, as onboarding, development, training, and retention are critical to building staff for the future and the emerging threats to the Nation.

A major challenge is envisioning what the cyber workforce will look like in the future, but we have learned a tremendous amount through our work with government officials and business executives. Booz Allen is at the forefront of what is required to build a comprehensive cyber workforce today and we are sharing our best practices with our clients worldwide.
When it comes to developing our cyber workforce, we can glean several key lessons from strategies we employ in tackling everyday cyber security challenges.

**Multi-Layered Strategy**

A single defense system is insufficient to keep a network secure. Likewise, a single talent development approach is not likely to keep your workforce on the cutting edge. A development program must blend and layer strategies for both training and delivery. Our people work in different locations, they keep different schedules, and they have different learning styles. A one-dimensional approach is not going to meet the needs of such a diverse workforce.

At Lockheed Martin, we offer a variety of live and online training options. And we offer tuition assistance for advanced degrees and certifications. Perhaps our most innovative approach is a mobile Cyber University — a cadre of professional trainers who lead cyber classes at locations around the country. Using a blended, layered approach, we provide employees options that fit their schedule, learning style and skill needs.

**People, Process and Technology**

Cyber security can't begin and end with technology. The people and processes that use and govern that technology are an integral part of any effective defense. The same holds true of workforce development. It is crucial to keep employees up-to-date on the latest technology trends in cyber. But it is just as important to teach them the people and process side of the equation. Teambuilding, leadership, critical thinking, and strategy are all key to building a successful workforce, just as developing the right processes to share knowledge is key to sustaining that workforce. Our Center for Leadership Excellence in Bethesda is designed to be an industry leadership factory, equipping our people with the full spectrum of skills they’ll need to take on our customers’ toughest challenges.

**Partnerships**

Cyber security teams must build partnerships with numerous stakeholders if they hope to succeed. Workforce development is no different. At Lockheed Martin, we’re partnering with the Anne Arundel Workforce Development Corporation, ISC2, SANS, Global Knowledge, Technodyne, IQShare and others to develop and deliver cyber training to local professionals. We forged a strategic partnership with the University of Maryland to conduct joint research & development, sharpen cyber curricula, and share plans and knowledge on future cyber challenges. We partner with the National Security Scholarship Program to fund college education and guide talented interns into government and industry careers. And we’re proud to partner with high schools across the Maryland region to ignite students’ interest in cyber careers.

But we know we can do more, and we call upon industry and government to launch the partnerships that will shape the future of our cyber workforce. We need a strong pipeline of cleared experts, a shared road map of requirements and hard problems, and a collaborative spirit that puts the mission first. Cyber security, like cyber workforce development, can only succeed with all of us working together towards a common goal.
Our nation faces a serious threat of supply and demand of cybersecurity professionals. The demands of government, academia and industry far exceed the supply of resources coming from high schools and higher learning institutions by multiple orders of magnitude. We need to better incorporate science, technology, engineering and mathematics (STEM) into primary and secondary education with the intent of increasing the number of cyber graduates that enter the workforce.

Science Applications International Corporation (SAIC) has invested millions of dollars in a diverse portfolio of outreach and STEM activities to help bolster the nation's cyber and engineering savvy future generations. Efforts include:

- Alliance programs with universities
- Cyber competitions at the high school, college and professional levels
- National Cyber Security Alliance for general cyber awareness
- Securing our eCity initiative, public-private partnerships to create a cyber-secure community
- FIRST Robotics
- Project Lead the Way®

Last year SAIC, the University of Maryland, Baltimore County (UMBC), TechCouncil of Maryland and the National Cyber Security Alliance (NCSA) teamed with the Office of Maryland Governor Martin O'Malley to host the inaugural Maryland Cyber Challenge and Conference as a continuation of our commitment to demonstrate shared cyber responsibility.

The dynamic nature of cyber trends, threats, and technology requires active cyber community engagement for SAIC employees. Thus, we have a presence on various boards and committees across associations, organizations and community boards focused on cyber-related topics. cybergamut is a community of practice SAIC sustains for industry, academic, and government professionals who work on cyber challenges. Over 1,500 cyber professionals from more than 300 organizations worldwide come together to share ongoing professional development opportunities, as well as engage in Technical Tuesday presentations. Technical Tuesday enables the exchange of ideas on technical issues of mutual interest, such as case studies in cyber attacks and modern forensic investigative techniques.

The most advanced cyber training will last only as long as skilled professionals stay sharp. SAIC's solution to this challenge is our CyberNEXS cyber training program that builds and exercises skills in secure configuration, intrusion detection, incident mitigation, penetration testing, and forensics through on-site or remote training against live, real-world cyber threats in a customizable environment.

Internally, SAIC recognized the increased need for cyber workforce modernization as a critical issue over three years ago. We embarked on an aggressive training and education program that is now an industry model. SAIC sent hundreds of employees through multiple cyber-oriented master's degree programs as well as multiple certification programs to equip employees with the knowledge and credentials necessary to comply with Department of Defense standards. We operate a very successful college internship program in Columbia, Md. Interns are integrated into current mission programs, research initiatives and development projects where they are mentored by experts and deliver value to our clients. Students complete the program with cyber experience and often clearances.

SAIC commends the Fort Meade Alliance for its leadership and continued dedication to this vital issue.

1. Project Lead The Way and PLTW are registered trademarks of Project Lead The Way, Inc. in the U.S. and/or other countries.
LG-TEK is a leading supporter of cyber and cybersecurity training. We are currently supporting these types of initiatives. Our corporate focus for training dollars is programmed as part of our overall educational support to our own employees for the continuation of their instructional skills in these fields.

LG-TEK employees who provide training in this field are able to attend specific cyber and cybersecurity-related conferences or symposiums to further their own understanding and allow them to have a better ability to provide cyber and cybersecurity training. Further, we believe that educators are addressing workforce needs at higher levels through the establishment of degree programs in the cyber and cybersecurity fields. At LG-TEK, we are involved in focus groups and working groups with educational institutions to help them better define the needs in cyber and cybersecurity fields. This results in a development of better programs for career fields in the cyber and cybersecurity arena.

Cyber is affecting our own hiring plans because we are reaching out to highly technical individuals with instructional experience who have the ability to develop a thorough understanding and expertise in key skills related to cyber and cybersecurity. This is critical to our own initiatives to provide the best possible instructional support in a classified environment.

LG-TEK works in the classified environment and we are providing cyber and cybersecurity training in this arena. We work with our customers in developing specialized cyber and cybersecurity programs for a classified environment.
The Fort Meade Alliance Salutes Our
Five-Star Members

AECOM
AEROTEK
Anne Arundel Community College
Anne Arundel Economic Development Corporation
Axom Technologies
Booz Allen Hamilton
Corporate Office Properties Trust
HP
L-3 Communications
LG-TEK
Lockheed Martin
M&T Bank
ManTech International Corporation
Merritt Construction Services
Northrop Grumman
Raytheon
SAIC
Software Process Technologies
TASC
TeleCommunication Systems
The SI
Whiteford, Taylor & Preston

The Fort Meade Alliance is funded, in part, by a grant from the Maryland Department of Business and Economic Development.