S. HRG. 112–262

# THE ROLE OF SMALL BUSINESSES IN STRENGTHENING CYBERSECURITY EFFORTS IN THE UNITED STATES

## HEARING

BEFORE THE

## COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JULY 25, 2011

Printed for the Committee on Small Business and Entrepreneurship

Available via the World Wide Web: http://www.fdsys.gov

U.S. GOVERNMENT PRINTING OFFICE

71–267 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP

ONE HUNDRED TWELFTH CONGRESS

---

MARY L. LANDRIEU, Louisiana, *Chair*
OLYMPIA J. SNOWE, Maine, *Ranking Member*

| | |
|---|---|
| CARL LEVIN, Michigan | DAVID VITTER, Louisiana |
| TOM HARKIN, Iowa | JAMES E. RISCH, Idaho |
| JOHN F. KERRY, Massachusetts | MARCO RUBIO, Florida |
| JOSEPH I. LIEBERMAN, Connecticut | RAND PAUL, Kentucky |
| MARIA CANTWELL, Washington | KELLY AYOTTE, New Hampshire |
| MARK L. PRYOR, Arkansas | MICHAEL B. ENZI, Wyoming |
| BENJAMIN L. CARDIN, Maryland | SCOTT P. BROWN, Massachusetts |
| JEANNE SHAHEEN, New Hampshire | JERRY MORAN, Kansas |
| KAY R. HAGAN, North Carolina | |

DONALD R. CRAVINS, JR., *Democratic Staff Director and Chief Counsel*
WALLACE K. HSUEH, *Republican Staff Director*

# C O N T E N T S

OPENING STATEMENTS



WITNESSES

**Panel 1**



**Panel 2**



ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

# THE ROLE OF SMALL BUSINESSES IN STRENGTHENING CYBERSECURITY EFFORTS IN THE UNITED STATES

**MONDAY, JULY 25, 2011**

UNITED STATES SENATE,
COMMITTEE ON SMALL BUSINESS
AND ENTREPRENEURSHIP
*Washington, DC.*

The Committee met, pursuant to notice, at 2:55 p.m., at the Laurel Municipal Center, City Council Chambers, 8103 Sandy Spring Road, Laurel, Maryland, Hon. Benjamin L. Cardin, presiding.

Present: Senators Cardin and Mikulski.

## OPENING STATEMENT OF THE HONORABLE BENJAMIN L. CARDIN, A UNITED STATES SENATOR FROM MARYLAND

Senator CARDIN. Good afternoon and welcome to the hearing of the Committee on Small Business of the United States Senate. I first want to thank Chairman Mary Landrieu, who is the Chairman of the Small Business Committee—I have the honor of serving on that Committee, for allowing me to conduct this hearing in Laurel, Maryland, on a very, very important subject to not only the small business community, but to our entire country, The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States.

I want to thank my colleague and friend, Senator Barbara Mikulski, for joining us today. Senator Mikulski, as I am sure you all are aware, serves on three very important committees, but two that are directly related to cybersecurity. One is on the Senate Intelligence Committee, the other on the Senate Appropriations Committee. She also serves on the Committee on Health, Education, Labor, and Pensions, which obviously is also an important Committee as it relates to the training of people in the cybersecurity area. So, Senator Mikulski, thank you for joining me today in this hearing.

I want to thank our friends from Laurel for allowing us to use this facility, Mayor Moe. Thank you very much. The Council people that are here. We very much appreciate your hospitality today. There could not be a better place for us to have this hearing. It is a growth area in Maryland and one that is very much connected to the cybersecurity issues.

I also want to acknowledge Delegate Susan Lee who is here. She chairs the committee, along with Senator DeGrange, on cybersecurity issues, a committee that was established by legislation that she helped author. So it is very nice to have you here,

Susan, and we look forward to working in partnership with our colleagues in the State Legislature.

Cybersecurity is an issue that is of utmost importance to our country. In the last Congress, I had the opportunity to chair the Subcommittee on the Judiciary Committee that dealt with Homeland Security, cybersecurity issues. And I mention that, because during the course of that chairmanship, I had the opportunity to learn firsthand of the risks to our country.

There are cyber criminals out there and I think we all know cyber criminals. But in addition, we also have cyber terrorists that are out there, people who are trying to do havoc to this nation through cyberspace to America. But there are also cyber soldiers, agents of other countries that are operating, that are trying to compromise America's security.

They can do this through—cyber criminals can, of course, do it by bank robberies that make the old bank robbers look like they are pikers compared to the danger that can be attached to our financial system. In a matter of just a few hours, millions of dollars were stolen in several countries through the ATM machines. So we know that cyber criminals are out there.

But cyber terrorists are really trying to cause havoc to this country. They are trying to compromise our security, trying to deal with our energy grids, trying to deal with our transportation grids. And we know that, other countries are interested in trying to compromise our defense strategies through cyber-attacks. So these are issues that are of utmost importance to our country.

I authored a bill, S. 372, which is aimed at cybersecurity and Internet safety standards by having the Government work with the private sector to develop best practices for protecting us from our vulnerability against cyber-attacks. That legislation is moving forward as an effort to figure out how we can do things better, which really brings me to the current subject of how we and the small business community and in Maryland can help solve a national problem as well as growing our own economy.

In Maryland, we are very proud as being what we call the Cyber Center for this nation. Governor O'Malley has called it Cyber Maryland, putting a strong focus on the cybersecurity issues in our State through the tools of the State government.

We are proud of the Federal agencies that are located here and the new U.S. Cyber Command. Fifty key security and intelligence facilities located in the State of Maryland, 12 major military installations in the State of Maryland, our colleges, our universities that have concentrated on cybersecurity issues.

There is a great deal of energy here in Maryland and we want that energy, to a large extent, focused on the small business community. We know that job growth in America will be through our small businesses. We know that we will get more innovation through small companies. That is where the energy level starts, and we need to do a better job in energizing our small business community.

In the Congress, we passed recently several bills to help small businesses. We know about the concerns, of those in Federal agencies, as to whether they are allocating fair dollars to the small business community. We know of the abuses of bundling small con-

tracts into large contracts, making it virtually impossible for a small company to get the prime contract.

We know of the frustration in a tough economy, as to whether the agencies have adequate staffing to be able to reach out beyond their current suppliers and contractors. We want to overcome those obstacles because we think it is critically important for job growth and innovation, to be able to make sure that the small business community is getting their fair share of the work, and we also understand the issues of credit.

Secretary Johansson, I am glad that you are here, because we are going to talk a little bit today about the efforts being made by Congress. Congress made significant resources available to ease up credit. Part was direct through the Federal Government; part was through the States, and I would be interested to hear the experiences in Maryland as it relates to getting resources out to small businesses in order to move this agenda forward.

At this time, let me yield to my colleague, Senator Mikulski, for her opening statement.

## OPENING STATEMENT OF HON. BARBARA A. MIKULSKI, A UNITED STATES SENATOR FROM MARYLAND

Senator MIKULSKI. Well, Senator Cardin, I want to thank you for hosting this hearing. Your championship of small business is well-known, and your persistent advocacy is much appreciated.

Like you, I join today to see how, in our effort to keep our country safe, particularly against the new enduring war of cyber war, we also want to build a safer and stronger economy by making sure that the money that we spend, both within Government and within the private sector, provides as much access as we can—not only to big business who often knows how to work the system, but to small- and medium-size businesses so that we can have a safer country—indeed, a stronger economy.

I am so proud of where Maryland is in this new enduring war. It is here that we are on the battleground to protect America. The key critical assets in both military and civilian agencies are right here in Maryland.

We truly are the epicenter of cybersecurity for the United States of America, and because of our unprecedented know-how in this area—particularly rested in the National Security Agency working with the National Institute of Standards and Technology—we are actually the epicenter, in many instances, for the world, at least for the free world that wants to remain free.

Just to list a few, to list, actually, the basic ones, of course, is what I affectionately call the "Mothership," the National Security Agency. That is the listening post for cyber and signals intelligence throughout the world, protecting our troops in Iraq and Afghanistan, whether it is a Navy Seal going to take down Bin Laden, or it is a plane over Libya, or whether it is keeping an eye on North Korea or any other bad guy whose name is even too unmentionable to bring up.

They are on the job 24/7. The National Security Agency is also the home to the Cyber Command. It is the job of the Cyber Command to protect .mil for the entire United States of America, and also be linked with treasured allies in its protection.

VerDate Nov 24 2008 13:44 Feb 21, 2012 Jkt 071267 PO 00000 Frm 00007 Fmt 6633 Sfmt 6633 C:\DOCS\71267.TXT DPROCT

And then we have special agencies: DISA, the Defense Intelligence Service Agency. The 10th Fleet that is there right now—a fleet like no other fleet. It does not have aircraft carriers. It does not have submarines. But boy does it have the Navy-Marine spirit in which their job is to protect the entire critical Naval assets.

And then, as we move out, because we always need new ideas in this new enduring war, there is IARPA, the Intelligence Advanced Research Projects Activity that is right next to College Park, for the synergistic effect with our intellectual capital at the universities, where they will develop the new ideas to protect not only .mil and .gov, but .com and individuals who are threatened every day.

And then, in order to come up with the new ideas, you need new products. You can't have new products without standards, and it is the National Institute of Standards and Technology, working with both government and the private sector, that is creating the standards so that we have interoperable products that protect us, but also protect our economy.

Well—you think I am a little excited about it?

But, listen, I know the "Mothership" alone spends $2.5 billion in contracts. So while I have extolled your virtues, I want you to tell me how you will open the doors of Government or you have them opened already, so that small business can compete on the basis of merit.

Senator Cardin: We do not give people contracts. What we do do is fight for the opportunity for them to go after the contracts based on their know-how, their ability, and the value that they offer to the United States Government.

So we look forward to hearing from you. But right now, I salute you because you are the front line warriors in this new and enduring war.

Senator CARDIN. Well, thank you very much, Senator Mikulski.

We will now go to our first panel. Let me welcome all three of our panelists. Dr. Patrick Gallagher was confirmed as the 14th Director of the U.S. Department of Commerce's National Institute of Standards and Technology, NIST, in 2009. He also serves as Under-Secretary of Commerce for Standards and Technology. Dr. Gallagher brings high level oversight and direction for NIST. The agency promotes U.S. innovation and industrial competitiveness by advancing measurements, science, standards, and technology. So we very much welcome you, Dr. Gallagher.

We will then hear from Jennifer Walsmith. Jennifer Walsmith has served as the Senior Acquisition Executive for the National Security Agency since January, 2009. In this role, she is responsible for all procurement in support of NSA's signals, intelligence, and information assurance missions. While managing the agency's multibillion dollar budget, as Senator Mikulski has pointed out—and Senator Mikulski is very much aware of that as one of the appropriators——

Senator MIKULSKI. That is open source, too.

Senator CARDIN. That is right. Ms. Walsmith has focused on balancing acquisition discipline with mission agility.

And then we will hear from our own DBED Secretary, Christian Johansson. He was appointed Secretary by Governor Martin

O'Malley in early 2009. He oversees Maryland's nearly 250 employee business agency and its $25.6 million budget. During his tenure, he has helped the Governor craft strategic plans, and informed councils targeting Maryland's competitive business trends in a rapidly changing industry such as biotech, cybersecurity, IT, and foreign direct investment.

All three of you, it is a pleasure to have you before the Committee and we will start with Mr. Gallagher.

## PANEL 1

### STATEMENT OF HON. PATRICK D. GALLAGHER, DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, UNITED STATES DEPARTMENT OF COMMERCE

Dr. GALLAGHER. Thank you very much, Senator Cardin and Senator Mikulski. It is a real pleasure to be here today to talk about cybersecurity in business. I want to start by thanking Team Maryland for your leadership on cybersecurity, for your recognition of its importance to the nation's security, and to its economic future, and for helping to make Maryland really the epicenter of this effort.

Mr. Chairman, I will focus my testimony today on the important interplay between the small business community and this cybersecurity effort. In my written testimony, I have some more information about these efforts that I will not be able to get into in this time, particularly the National Initiative on Cybersecurity Education and the Proposed National Cybersecurity Center of Excellence championed by Senator Mikulski. Both of these efforts will also benefit the small business community.

More than 99 percent of all U.S. businesses are small and medium size enterprises. Small businesses are the growth engine of our economy, and they account for most of the new job creation in this country. Information technology has brought huge advantages to these businesses, but they also face significant threats and unique vulnerabilities caused by their size and diverse organizations.

In fact, it has been recently reported that data and identify theft are impacting small and medium size businesses at a rate greater than of individuals. Many of these businesses house very sensitive personal, health care related, or financial information. Many small businesses also provide direct services to our Federal, State, local, and tribal governments, and therefore, have access to government information or systems.

In this interconnected environment, it is vital that small businesses be aware of the risks and take appropriate steps to ensure that their systems are secure. And given their critical role, a vulnerability common to the small business community could pose a significant overall threat to this nation's economy or national security.

NIST programs work with industry to set the standards that protect businesses of all sizes, as well as the Federal Government, from cyber threats. Our efforts are broad and include cybersecurity research, standards, developing the tools and tests to demonstrate conformance with standards, guidance documents, and cybersecurity outreach and education.

VerDate Nov 24 2008 13:44 Feb 21, 2012 Jkt 071267 PO 00000 Frm 00009 Fmt 6633 Sfmt 6633 C:\DOCS\71267.TXT DPROCT

Today I would like to focus on just two areas of critical importance to the small business community, identify management through the National Strategy for Trusted Identifies in Cyberspace, or NSTIC, and cloud computing.

So NSTIC was announced in April of this year at an event that I had the pleasure of joining Senator Mikulski with, and this program seeks to better protect consumers from fraud and identity theft, to enhance individuals' privacy, and to foster economic growth by enabling industry, both to move more services online and to create innovative new services.

This strategy aims to make online transactions more trustworthy and give businesses and consumers both the confidence they need to work online. The Federal Government's efforts in this public/private effort will be led by NIST. Our job is to facilitate the development of interoperability technology standards and policies, and create an identity ecosystem where individuals, organizations, and the underlying infrastructure such as routers and servers, can be authoritatively authenticated.

Small businesses will be able to use this infrastructure to avoid the cost of building their own cumbersome log-in systems and take their business online and reduce the cost to both themselves, and make the user experience more convenient for their consumers. It can also expand their ability to reach out to new consumers across the nation and around the world.

Similarly, cloud computing and its growth offers a unique opportunity for small businesses in all sectors to make use of powerful computing resources without requiring up-front or long-term IT investment. Small businesses can contract and use computing services through the cloud computing model and only pay for those resources that they choose to use and actually consume, and the model is providing a path for small businesses and others to be able to easily move data systems from one cloud provider to another.

It is for these very reasons that the Federal Chief Information Officer is determined that it helps the Government, too. And under the Cloud First Strategy, NIST has been tasked with working with the business community to develop the shared requirements, standards, and best practices to promote adoption of the cloud computing in a way that continues to ensure privacy, security of data in the cloud, and ensures that cloud services are interoperable, portable, and reliable.

Small businesses play a special role in the NIST programs. This is because they provide the critical technical competencies that allow us to do our work. It is by harvesting their entrepreneurial spirit and innovative capacity that NIST is able to integrate cybersecurity standards and safeguards in a meaningful way into the technology that our nation depends on.

In short, we cannot accomplish our mission at NIST without this community. So I want to thank you for the opportunity of appearing before this Committee and I am happy to answer any questions.

[The prepared statement of Mr. Gallagher follows:]

# Testimony of

# Patrick D. Gallagher

# Director

# National Institute of Standards and Technology

# U.S. Department of Commerce

# before the

# Committee on Small Business and

# Entrepreneurship

# U.S. Senate

# "The Role of Small Businesses in Strengthening

# Cybersecurity Efforts in the United States"

# July 25, 2011

**Introduction**

Senator Cardin, members of the Committee, I am Patrick Gallagher, Director of the National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce. Thank you for this opportunity to testify today on our perspective regarding the "The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States." We recognize that small businesses play an important role in the U.S. economy. Since use of the Internet is critical in the delivery of goods and services for all businesses, the importance of addressing risks associated with doing business in a cyber environment cannot be overstated. Today I will focus my testimony on the role small businesses are playing in helping the U.S. Government strengthen our cybersecurity efforts and programs, as well as providing information on NIST's cybersecurity programs and activities that can assist small businesses.

Ensuring that business related information is secure is essential to the functioning of our economy -- and indeed to our democracy. Small businesses, like all organizations, want to embrace and have available the latest advances in technology to make their tasks easier, improve productivity, and remain competitive. But they face an enormous challenge in protecting their information in a cyber environment. In fact, it was recently reported[1] that data and identity theft are impacting small and medium-sized businesses more than individuals.

More than 99 percent of all U.S. businesses are small or medium-sized2; a vulnerability common to a large percentage of these organizations could pose a significant threat to the Nation's economy and overall security. Many of these businesses house very sensitive personal information, including healthcare or financial information. Many small businesses also provide services to our federal, state, local and tribal governments and have access to government information or systems. In the interconnected environment in which we all operate, it is vital that this important sector of our economy be aware of the risks and take appropriate steps to ensure their systems are secure. As described in the Department of Commerce's Internet Policy Task Force's paper, *Cybersecurity, Innovation and the Internet Economy,* the rapid development and implementation of sector-specific, consensus-based codes of conduct is critical to protecting the Internet and information innovation sector (I3S) from cybersecurity threats. Through the leadership of NIST and other bureaus, the Department of Commerce can play an important role to convene the I3S and related sectors and industries and facilitate their development of voluntary codes of conduct. Where sectors (such as those with a large number of small businesses) lack the capacity to establish their own voluntary codes of conduct, new and existing NIST guidelines would be available to bridge gaps in security protection.

When implementing new technologies, small businesses need to fully understand all of the potential security risks created by connecting to the Internet. Indeed, the risks to our systems are so complex and pervasive, that we cannot reasonably expect small businesses

[1] "Cybercrime Losses Among SMBs Reach New Highs In Study," http://www.darkreading.com/smb-security/167901073/security/privacy/229402972/cybercrime-losses-among-smbs-reach-new-highs-in-study.html.

[2] "How important are small businesses to the U.S. economy?," http://www.sba.gov/advocacy/7495/8420

to be experts in all areas of security, including properly implementing security controls for complex system configurations and assessing security features associated with new and emerging technology. It is critical that small business needs and requirements are considered as cybersecurity standards and guidelines are developed.

NIST's mission in cybersecurity is to work with federal agencies, industry, and academia to research, develop and deploy information security standards and technology to protect information systems against threats to the confidentiality, integrity and availability of information and services. Consistent with this mission and with the recommendations of the President's *Cyberspace Policy Review*, NIST is actively engaged with private industry, academia, non-national security federal departments and agencies, the intelligence community, and other elements of the law enforcement and national security communities in coordination and prioritization of cybersecurity research, standards development, standards conformance demonstration and cybersecurity education and outreach activities. Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users – from small and medium enterprises to large private and public organizations including agencies of the federal government.

**NIST's Current Statutory Responsibilities under FISMA**

The Federal Information Security Management Act (FISMA), Section 303, states that NIST shall:

- have the mission of developing standards, guidelines, and associated methods and techniques for information systems;
- develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency, other than national security systems; and
- develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems.

While targeted primarily toward federal agencies, the FISMA security standards and guidelines also are used widely by other organizations, including small businesses to help ensure that the information systems supporting enterprise operations are well protected, thereby enhancing competitiveness and productivity.

A sample of some NIST guidance which is available to small businesses is listed below:

- Small Business Information Security: The Fundamentals;
- Guide for Securing Microsoft Windows XP Systems;
- Wireless Network Security;
- Security Considerations for Voice Over IP Systems;
- Guidelines on Electronic Mail Security;
- Guidelines on Securing Public Web Servers;
- Guidelines on Firewalls and Firewall Policy;
- Procedures for Handling Security Patches;
- Contingency Planning Guide for Information Technology Systems;
- Guidelines on Cell Phone and PDA Security;
- Risk Management Guide for Information Technology Systems.

All of these documents, as well as our ITL Bulletins, are available on our web-based Computer Security Resource Center (CSRC) (http://csrc.nist.gov) which provides a wide range of security materials and information to all. CSRC now has over 20 million "hits" annually. The CSRC site also contains many policies, procedures, and practices from both federal agencies and the private sector that are also advertised to the public through NIST's publications and outreach efforts.

We have developed guidance for organizations, large and small, to maximize the security of their information systems so that they may securely conduct business transactions over the Internet. Hardware and software purchased by small businesses today are frequently installed with the original configurations delivered by the vendor, which can often lead to vulnerabilities or other security weaknesses. We are helping small businesses to understand security features and the importance of correct configuration. Even if they have taken steps to minimize the opportunity for inappropriate access by investing in firewall technology and virus protection software, they need to ensure that these technologies are correctly installed, managed, and updated regularly. NIST also created a video that explores the reasons small businesses need to secure their data: http://www.youtube.com/watch?v=ajwX-7jVLo0&feature=player_embedded
Given the state of software insecurity today, vendors frequently issue security patches for their products. Through our outreach efforts, we are advising users of the importance of these patches and where to get up-to-date information and procedures for installing patches.

**Interagency Collaborations**
In 2002, NIST partnered with the Small Business Administration (SBA) and the Federal Bureau of Investigation's InfraGard program to sponsor computer security workshops and provide online support for small businesses. The workshops, which are held across the country, feature security experts who explain information security threats and vulnerabilities and describe protective tools and techniques which can be used to address potential security problems. Since May 2010, we have held 24 workshops in 22 cities with 1105 small business owners and employees attending. To expand our outreach efforts, NIST has also developed a Small Business Outreach Site (http://csrc.nist.gov/securebiz/) for easy access to security resources and to provide small businesses with the ability to request a workshop to be held in a specific local area.

For the last four years NIST, in cooperation with SBA and the Association for Small Business Development Centers, has participated in the annual conference of Small Business Development Centers, providing participants with information to increase awareness of NIST resources. NIST is also working with the National Cyber Security Alliance (NCSA) to help make cybersecurity a priority for small businesses (http://www.staysafeonline.org/for-business).

**National Initiative for Cybersecurity Education**
The National Initiative for Cybersecurity Education (NICE) represents the evolution of the cybersecurity education component of the Comprehensive National Cybersecurity

Initiative (CNCI), expanding it from a federal focus to a larger national focus. NICE was created to meet the cybersecurity training, education, and awareness priorities expressed in Chapter II, Building Capacity for a Digital Nation, of the President's Cyberspace Policy Review[3]. It will enhance the overall cybersecurity posture of the U.S. by accelerating the availability of educational and training resources designed to improve the cyber behavior, skills, and knowledge of every segment of the population, enabling a safer cyberspace for all. The effort is for all U.S. citizens of all ages (pre-school to senior citizens), and all types of professions whether it be in academia (pre-school, K-12, college/universities), federal/state/local government, business (small-medium to large size businesses/companies), or local community group or non-profit organization. The Strategic Plan for NICE will be available for public review and comment in late summer of 2011.

**Security Automation**

Through the development and adoption of data standards and specifications, security automation harmonizes the vast amount of Information Technology (IT) data into coherent, comparable information streams that inform timely and active management of diverse IT systems. Through the creation of internationally recognized, flexible, and open standards, security automation results in IT infrastructure interoperability, broad acceptance and adoption, improved situational awareness, and creates opportunities for innovation. Security automation standards currently support several initiatives, including widely used configuration checklists and the National Vulnerability Database. These standardized data sources provide a level playing field for security tool developers with innovative ideas, regardless of company size. Commercial off-the-shelf security automation tools also support cost-effective security management for small businesses that lack full-time IT security staff.

**IT Product Security Configuration Checklists**

IT products are often intended for a wide variety of audiences, so restrictive security configuration controls are usually not enabled by default. As a result, many out-of-the-box IT products are immediately vulnerable. In addition, identifying a reasonable set of security settings that achieve balanced risk management is a complicated, arduous, and time-consuming task, even for experienced system administrators. In order to alleviate some of the burden on all users, and in response to the Cyber Security Research and Development Act of 2002, NIST is facilitating the development and sharing of checklists that indicate settings and optional selections that minimize the security risks associated with computer hardware or software systems. NIST is providing a formal framework for checklist developers to submit checklists to NIST and publishing the checklists for easy access (http://checklists.nist.gov). There are currently more than 175 checklists posted on the website, including, but not limited to, checklists for Internet Explorer 7.0, Internet Explorer 8.0, Microsoft Office 2007, Red Hat Enterprise Linux, Windows 7, Windows Vista, and Windows XP. The checklists, when combined with high-quality guidance and training, substantially reduce the vulnerability of IT systems to attack.

---

[3] May 29, 2009, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

**National Vulnerability Database**
The National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data. Through NVD, NIST is providing relevant and important information in the area of vulnerability management. Currently the NVD contains information on nearly 47,000 vulnerability advisories with an average of 10 new vulnerabilities added daily. The NVD is relied upon by security tool vendors and end users in both the public and private sectors and is used by the Payment Card Industry Digital Security Standard to help identify key areas of risk within payment card systems.

**Software Quality**
Small and medium-sized businesses, indeed all organizations, rely on the software used on their information systems. NIST continues to work with industry to improve the security and reliability of software in a variety of domains. For example, we develop standards and test suites for interoperable, robust, quality web applications and products. Our test suites are being used throughout the industry to improve the quality of implementations and specifications. We develop ways to measure the effectiveness of software assurance tools, and conduct research to assess current methods and tools in order to identify problems that ultimately lead to software product failures and vulnerabilities. We conduct research and development in new areas to improve the quality of software, including software trustworthiness. We work with health-related organizations to advance the deployment of electronic health records and to facilitate the development and implementation of a nationwide health information network by developing robust software testing strategies.

**National Strategy for Trusted Identities in Cyberspace**
As with others, it is critical to small businesses that online services are provided in a secure, trustworthy manner. The recently released "National Strategy for Trusted Identities in Cyberspace[4]," lays out the vision for individuals and organizations, large and small, to be able to utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. The Strategy calls for a National Program Office to facilitate the carrying out of the Strategy and the development of interoperable technology standards and policies — an "Identity Ecosystem" — where individuals, organizations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. The goals of the Strategy are to promote private sector capabilities for protecting individuals, businesses, and public agencies from the high costs of cyber crimes like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas in a privacy enhancing manner.

The National Program Office (NPO), to be established within the Department of Commerce, will coordinate the federal activities – including coordination of cooperative public/private efforts - needed to implement NSTIC. The office will be led by NIST with activities involving public policy development and privacy protections to be led by the National

[4] April 15, 2011, *The **National Strategy for Trusted Identities in Cyberspace,*** http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

Telecommunications and Information Administration. The NPO will have full access to NIST technical expertise, both in the development and acceptance of broad consensus-based standards. NIST has been actively involved in the development and interoperability of secure identity management for many years and recently initiated research into how to make such identity schemes easy to use and hard to misuse.

**Cloud Computing**

The NIST Cloud Computing program is working with U.S. federal, state and local governments, industry, academia, standards development organizations, and the international community to help identify and develop standards that are needed to keep an open and level playing field for organizations of all sizes in this emerging technology field. NIST is also working to identify and help develop the guidance and technology needed to help organizations and individuals who use cloud computing services to do so securely and effectively. Finally, NIST, through its collaborative initiative to build a US Government (USG) Cloud Computing Technology Roadmap, is helping identify and develop the standards, guidance, and technology that USG agencies need to further adopt the cloud computing model to support their missions more cost effectively, securely, and with improved services. This helps small business on several levels -- directly by helping agencies improve services for small businesses, and indirectly by helping the US government to do its part in encouraging the development of the economically powerful cloud computing model.

The growing development and adoption of the Cloud Computing model supports small businesses on several fronts. It offers an opportunity for small businesses in all sectors to make use of powerful computing resources without requiring an upfront or long-term IT investment in equipment, software, or specialized IT people resources. Small businesses can contract and use computing services through the cloud computing model on a trial basis and only pay for the computing resources they choose to and actually consume. The model is also providing a path for small businesses and others to be able to easily move data and systems from one cloud provider to another.

The emerging Cloud Computing model also offers opportunities for IT sector firms of all sizes by providing cost effective infrastructure and application development platforms, making it easier for innovators and start up firms to enter the IT industry.

**Security Focused Research**

NIST's near-term effort in Internet security research is directed at working with industry and other government agencies to improve the interoperability, scalability, and performance of new Internet security systems, to expedite the development of Internet infrastructure protection technologies, and to protect the core infrastructure of the Internet.

Looking further into the future, we see the potential for new computational models, such as quantum computing, to threaten the mathematical underpinnings of today's cryptographic systems. In response, NIST is conducting research in the use of quantum information theory to devise network security technologies that do not depend on today's cryptographic techniques. NIST is a key player in the research and development of

biometric standards and systems. We are working with industry and other government agencies to improve the accuracy of biometric systems that utilize fingerprints, face, iris and multi-modal technologies.

With a highly mobile workforce, use of mobile devices is quickly becoming a necessity for small and large organizations. NIST is working in collaboration with industry to improve authentication and encryption techniques associated with these products to ensure that the user's data and wireless communications are protected.

Meeting the challenge of securing our Nation's IT infrastructure demands a greater emphasis on the development of security-related metrics, models, datasets, and testbeds so that new products and best practices can be evaluated. The President's FY 2012 Budget will support NIST's collaborations with industry and academia to develop the necessary metrics and measurement techniques that will be combined to provide an assessment of overall system vulnerability. Utilizing approaches that have been successful in characterizing effects in the physical systems, NIST will develop the necessary measurement science and technologies to secure the Nation's IT Infrastructure.

**Small Business support of NIST Cybersecurity Programs**

The sharing of cybersecurity standards and practices is more than just a one-way information flow from NIST to the small business community. Through our contracting and acquisition programs, NIST actively engages small business. Important examples of the contributions of small businesses include research, standards support, and products. Small businesses play an important role in NIST's identity and access management research and standards development activities and in determining usability factors that broaden the applicability and improve the effectiveness of security technologies. Small business is a key engine for innovation in the field of cybersecurity. Small business provides critical technical competencies in cutting-edge IT security tools, techniques and test capabilities that permit NIST to leverage their expertise in integrating cybersecurity standards and safeguards into some of our Nation's most critical initiatives, including the development of a secure and interoperable Smart Grid, the adoption of Health Information Technology, and the advancement of automated security vulnerability, asset, and configuration management. As small businesses expand their expertise into new sectors through their relationship with NIST, new opportunities for growth are created.

In addition, NIST relies on small businesses to directly and indirectly support its operational cybersecurity program. Directly, NIST relies on small business contractor labor to assist with the protection of NIST systems and assist with the formal cybersecurity assessment and authorization of NIST systems as required by OMB A-130 and FISMA. Directly and indirectly, NIST relies on small businesses to provide IT support services, such as help desk, out-of-hours system monitoring, desktop and server support, and application development which all play a critical role in protecting NIST computers, networks and information. NIST has also worked closely with small businesses that provide externally hosted applications and services used to support NIST's mission, assessing their security controls against FISMA requirements and

making recommendations on how to improve or implement specific controls to best protect sensitive NIST information processed by their applications and services.

**Conclusion**

In summary, Mr. Chairman, the IT security challenge facing small businesses is greater than it ever has been. Systems managed by small businesses are part of a large, interconnected community enabled by extensive networks and increased computing power. Certainly, there is great potential for malicious activity against non-secured or poorly secured systems or for accidental unauthorized disclosure of sensitive information or breach of privacy.

NIST will continue to develop ways to assist small businesses in their efforts to maximize capabilities and efficiencies offered by emerging technology while minimizing risk to their systems and information. We will continue our work in the areas of trusted identities, secure configuration settings, product benchmarks, outreach, training, and research. The President's FY 2012 Budget will enhance these efforts.

We believe the programs and activities described today demonstrate our commitment to a more effective national cyber security environment by assisting small enterprises in protecting their assets and staying competitive in a cyber economy.

Thank you, Mr. Chairman for the opportunity to present NIST's views regarding security challenges facing small enterprises. I will be pleased to answer any questions that you and the other members of the Committee may have.

## Patrick D. Gallagher

Dr. Patrick Gallagher was confirmed as the 14th Director of the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) on Nov. 5, 2009. He also serves as Under Secretary of Commerce for Standards and Technology, a new position created in the America COMPETES Reauthorization Act of 2010, signed by President Obama on Jan. 4, 2011.

Gallagher provides high-level oversight and direction for NIST. The agency promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. NIST's FY 2011 resources include $750.1 million from the Department of Defense and Full-Year Continuing Appropriations Act, 2011 (Public Law 112-10), $48.6 million in service fees, and $135.6 million from other agencies. The agency employs about 2,900 scientists, engineers, technicians, support staff, and administrative personnel at two main locations in Gaithersburg, Md., and Boulder, Colo.

Gallagher had served as Deputy Director since 2008. Prior to that, he served for four years as Director of the NIST Center for Neutron Research (NCNR), a national user facility for neutron scattering on the NIST Gaithersburg campus. The NCNR provides a broad range of neutron diffraction and spectroscopy capability with thermal and cold neutron beams and is presently the nation's most used facility of this type. Gallagher received his Ph.D. in Physics at the University of Pittsburgh in 1991. His research interests include neutron and X-ray instrumentation and studies of soft condensed matter systems such as liquids, polymers, and gels. In 2000, Gallagher was a NIST agency representative at the National Science and Technology Council (NSTC). He has been active in the area of U.S. policy for scientific user facilities and was chair of the Interagency Working Group on neutron and light source facilities under the Office of Science and Technology Policy. Currently, he serves as co-chair of the Standards Subcommittee under the White House National Science and Technology Council.

Senator CARDIN. Thank you very much for your testimony. Ms. Walsmith.

**STATEMENT OF JENNIFER S. WALSMITH, SENIOR ACQUISITION EXECUTIVE, NATIONAL SECURITY AGENCY, UNITED STATES DEPARTMENT OF DEFENSE**

Ms. WALSMITH. Good afternoon. Thank you, Senator Cardin and Senator Mikulski. Thank you. I appreciate the opportunity to talk with you both and the Committee on such a topic of vital importance, the role of small business and the role that they play in the success of our agency's mission.

If there was one thing that I could leave you with is the importance that we place on outreach to small business and giving them the opportunities that Senator Mikulski referred to earlier that is vital to our success and vital to our partnerships that we set forth with those businesses.

Cybersecurity, the protection and defense of our information systems, relies heavily, as you know, on technology. Small businesses play a role that no other can play in that regard. They have the agility and the innovation to create and deploy cyber products and services that are customized to NSA's missions needs through innovation and collaboration.

NSA engages in a variety of activities to promote partnership opportunities with small businesses and networks with industrial organizations that focus on supporting our agency's missions. Some of these agencies or organizations that we network with include AFCEA, American Small Business Coalition, Chesapeake Innovation Center, Chesapeake Regional Tech Council, and the Fort Meade Alliance.

NSA has developed an acquisition communication tool at our Acquisition Research Center that facilitates such communication between NSA and industry. Currently there are over 2,700 Maryland businesses registered in the ARC of which over 82 percent of them are small businesses. NSA uses the ARC to perform our market research and provide those opportunities to identify potential bidders for our efforts.

Our Office of Small Business Programs ensures that small businesses, including service-disabled veterans owned businesses (SDVOB) and HUBZone, all have the opportunity to participate in our acquisitions. The Department of Defense small business performance goal for NSA is 25 percent of prime contract dollars. As of 30 June 2011, NSA's small business performance was just over 17 percent.

We are working diligently to increase our small business utilization and NSA includes small business subcontracting requirements in our large contracts, of which we tie to award fee to ensure their utilization. This is very significant. It results in a significant amount of dollars to small businesses.

For example, in FY10, one of our prime contractors subcontracted more than 60 percent of the work to small businesses. In that single contract alone, it represented over $100 million to small businesses. This is a consistent trend in our large contracts.

There are many other positive trends within our small business area. Two that I want to mention briefly today are the utilization

of our SDVOB and HUBZone small businesses. We put a particular effort on this in 2008 to grow these two vital areas of business.

To just demonstrate the growth that we have seen in 2008, we had .3 percent in SDVOB. When we closed FY10, we had 1.53 percent of our appropriated dollars were awarded to prime contracts with SDVOB companies. This represents a five times increase in those prime contracts.

HUBZone is a similar story. We have increased that amount by 93 percent between FY09 and FY10. These trends demonstrate NSA's commitment to creating set-aside opportunities for small businesses. We have a variety of programs to increase the opportunity and the dialogue with small businesses.

We all know the chicken and egg that comes with classified contracting. If you do not have a security clearance, then you are often unable to break those barriers to understand what our business is all about. With that, we introduced a program we call the Provisional Industrial Security Approval Program, and what it does is it allows us to clear a set number of individuals from companies that wish to do business with us to allow for the technical conversations and the business development opportunities, and later allow them to compete on our contracts.

I'll take a moment to also talk to you about several other initiatives that we have specifically geared to small businesses. We have a large NSA set-aside called the NSETS Program, which enables us to competitively acquire agency requirements from a team of highly qualified small businesses. In the first three quarters of FY11, NSETS awarded over $133 million to small businesses.

NSA provides and participates in a number of outreach programs ranging from hosting large symposiums to small business interactions facilitating one-on-one capabilities briefings to promote their capabilities to individuals within our organization.

In the first three quarters of this year, NSA hosted over 28 technology expositions which demonstrated and allowed small businesses the opportunity to come directly into our spaces and share their capabilities with NSA personnel. Each event hosted over 20 to 25 companies and vendors had the opportunity to interact with over 300 to 400 agency personnel.

While that is just a single way for them to interact and show their capabilities, we also hosted several niche events this year, focusing on cloud computing, cybersecurity, wireless technology, and many others.

NSA offers a biweekly pathway to success and which is designed to educate small businesses on how to do business with NSA. We know that is a tough area. Getting to know us and knowing how to move into our market is not easy for a new business just getting started.

In the first three quarters of FY11, more than 650 businesses participated in our briefings. We hosted over four major events to promote activities that help them understand our upcoming competitive opportunities. These events collectively attracted over 1,700 businesses to interact with us.

In addition, because it all is so much of how you get to know us, we participate with speakers and subject matter experts in many

regional and national conferences all designed for people to begin to understand our agency better.

Through the above-mentioned programs and our outreach events, NSA programs connect with thousands of small businesses a year in an effort to promote small business opportunities to partner with NSA. Without them, we could not achieve our agency's mission. I look forward to your questions and this opportunity to speak with you today.

[The prepared statement of Ms. Walsmith follows:]

Statement for the Record of
Jennifer Walsmith, Senior Acquisition Executive
National Security Agency


Before the Senate Small Business Committee
On NSA's Outreach to Small Business for Cyber Security

July 25, 2011

Good afternoon, Chairman Cardin and distinguished members of the Senate Small Business Committee. My name is Jennifer Walsmith and I am the National Security Agency's (NSA) Senior Acquisition Executive (SAE). I appreciate the opportunity to be here today to talk briefly about NSA's outreach to the small business community to support cyber security. The small business community plays an important and integral role in strengthening our cyber security efforts and programs.

Cyber Security – the protection and defense of information and information systems – relies heavily on computer systems design and small business is key in this area. Small businesses have the agility to create and deploy cyber security products and services customized to meet NSA's mission needs through innovation and collaboration. NSA supports small business cyber innovation through partnerships with the Chesapeake Innovation Center, higher education institutions, and others to ensure the creation of the skills and products needed to protect and defend NSA's information and information systems. In addition, NSA engages in a variety of activities to promote partnership opportunities with small businesses and networks with industry organizations that focus on supporting NSA, including in the area of cyber security.

Some of the organizations with which we network include the Armed Forces Communication and Electronics Association (AFCEA) Central Maryland Chapter, American Small Business Coalition, Chesapeake Innovation Center, Chesapeake Regional Tech Council, Fort Meade Alliance, Information Assurance Small Business Association, Maryland Marketing Meeting and many others. Finally, NSA has an acquisition communication tool – the Acquisition Resource Center (ARC) – that allows communication between NSA and Industry. Using the ARC, Acquisition personnel perform market research for each effort within NSA to determine vendors that have the technical requirements for award. In the State of Maryland, of the 2,754 businesses that are registered in the ARC, 2,253 (82%) are small businesses. NSA recognizes the importance of industry partnerships to achieve our mission and provides programs and outreach activities to ensure maximum practicable prime and sub contracting opportunities for small business concerns to participate in NSA acquisitions.

The mission of the NSA Office of Small Business Programs (OSBP) is to ensure that small businesses, including veteran-owned, service-disabled veteran-owned (SDVOSB), historically underutilized business zone (HUBZone), disadvantaged, and women-owned concerns have maximum practicable opportunity to participate in NSA acquisitions. The Department of Defense small business performance goal for NSA is 25% of prime contract dollars. As of June 30, 2011, NSA's small business performance is 17.33%. We are working diligently to increase our small business utilization. NSA includes small business subcontracting requirements in our large contracts and ties award fees to ensure small business utilization. This results in a significant amount of dollars to small business. For example, in FY 2010, one of NSA's prime contractors subcontracted more than 60% of its contract dollars, and of that subcontracted amount, more than 60% went to small business concerns – representing more than $100 million to small businesses. That is just one of our large contractors. This is a consistent trend in our large contracts. There are many other positive trends within specific small business concerns; two such trends are increased utilization of SDVOSB and HUBZone small businesses. In FY 2008, NSA's SDVOSB utilization was 0.3%, which increased to 0.8% in FY 2009 and to

1.53% in FY 2010. HUBZone prime contract dollars increased by 0.93% from FY 2009 to FY 2010. These trends demonstrate NSA's commitment to creating set aside opportunities for small business. NSA offers a variety of programs to increase small business participation in NSA acquisitions. These initiatives include: the Provisional Industrial Security Approval and NSA Set-Aside for Small Businesses II programs, which I will discuss more in a moment, Technology Expos/Vendor Showcases, Pathway to Success briefings, Agency-sponsored events, and participation in Industry events.

The NSA Provisional Industrial Security Approval (PISA) program provides an avenue for small businesses to receive personnel clearances to engage in classified business development discussions with NSA personnel; one hundred small businesses have been added to the PISA program in the first three quarters of FY 2011. More than 50% of the 1,135 PISA program participants have received NSA contracts since the program's inception in FY 2005. We also manage the NSA Set-Aside for Small Businesses (NSETS II) program which enables us to competitively acquire agency requirements from teams of highly qualified small businesses. In the first three quarters of FY 2011, the NSETS II program has provided $133 million worth of contracts to small businesses.

NSA provides and participates in a variety of outreach programs ranging from hosting large symposiums to educating small business on upcoming NSA mission and acquisition needs, to facilitating one-on-one capability briefings for small businesses to promote their capabilities to NSA personnel. In the first three quarters of FY 2011, NSA hosted 28 Technology Expos/Vendor Showcases which provided small businesses the opportunity to promote their capabilities at NSA locations to Agency personnel. Each of these events average 20-25 small businesses vendors and 350-400 agency employees. While Technology Expos/Vendor Showcases focus on the small business community at large, we also provided several niche events this year around the following themes: cloud computing, cyber security, wireless technology, signals intelligence, and veteran-owned/service disabled veteran-owned small businesses.

NSA offers a biweekly Pathway to Success briefing which is designed to educate small businesses on how to do business with NSA. In the first three quarters of FY 2011, more than 650 businesses participated in our 13 briefings. NSA hosted four major events in FY 2011 to promote agency activities to our industrial base. These events collectively attracted more than 1750 business representatives and included: NSA Acquisition and Industry Symposium (NAIS); NSA Acquisition/Industry Partnership Exchange (NAIPE), Business in a Minute, and the NSA/AFCEA Mission and Acquisition Symposium (NAMAS). NAIS, held November 2, 2010, provided an interactive forum for the 520 attendees, 50% of which were small businesses, to develop and strengthen partnerships between NSA and Industry. NAIPE, held January 20, 2011, connected 280 industry representatives with Agency personnel to discuss a variety of issues encountered while partnering together to meet NSA's mission and goals. Business in a Minute, NSA's largest unclassified event, was held April 4, 2011, and fostered Industry/NSA relationships by facilitating face-to-face meetings between the 370 business attendees and 180 NSA/Prime Contractors hosts. During the course of the event, more than 1000 meetings were held for small businesses interested in doing business with NSA. NAMAS, held May 3-4, 2011, attracted more than 580 industry guests and provided current and upcoming NSA acquisition

information to support industrial forecasting and strategic business planning in an effort to increase and strengthen partnerships between NSA and Industry.

NSA also regularly and actively participates in industry hosted events with organizations such as: AFCEA Central Maryland Chapter, Maryland Marketing Meetings, BRAC Business Initiative, Chesapeake Regional Tech Council, Maryland Department of Business and Economic Development (DBED), etc., to network amongst small businesses that are working with or desire to work with NSA.

In addition, NSA provides speakers and subject matter experts for regional and national conferences in an effort to promote doing business with NSA. During FY 2011, NSA has participated in: the 2011 Mentor Protégé Conference in Virginia Beach, the Smart Proc and Cyber Security conferences hosted by Congressman Bartlett in Ft. Detrick, Maryland, DBED events, the Ft. Belvoir Procurement Fair and Meeting, the RSA Conference in San Francisco, the 2011 DIA Conference in Miami, and the 2011 Detroit Small Business Defense Procurement Summit. In addition, we will participate in the upcoming Elite Veterans conference in Chicago and the National Veterans Small Business Conference in New Orleans.

Through the above mentioned programs and outreach efforts, NSA programs connect with thousands of small businesses each year in an effort to promote small business opportunities to partner with NSA to achieve our cyber security mission. I look forward to your questions.

**Jennifer S. Walsmith**
**National Security Agency Senior Acquisition Executive**

Ms. Walsmith has served as the Senior Acquisition Executive (SAE) for the National Security Agency (NSA) since January 2006. In this role, she is responsible for all procurements in support of NSA's Signals Intelligence and Information Assurance missions NSA. While managing the Agency's multi-billion dollar budget, she has focused on balancing acquisition discipline with mission agility. She has also placed a strong focus on leveraging industry expertise to maintain NSA's technological advantage.

Ms. Walsmith served in numerous positions in both industry and government throughout her career. After beginning as a Computer Systems Analysts at NSA, she joined private industry, where she managed several large software and database development efforts. Ms. Walsmith returned to the government in 1998 to serve as the National Reconnaissance Office (NRO) Director of Acquisitions and Corporate Decisions Group. She subsequently returned to NSA, where she has held several positions of increasing responsibility within the Agency's Acquisition Directorate. Prior to becoming the SAE, she served as the Deputy SAE and the Deputy for NSA's first Program Executive Office (PEO).

Ms. Walsmith holds a BS in Computer Science from the University of Maryland Baltimore County and is DAWIA Level III Certified in Program Management and a member of the Acquisition Corps. She resides in Annapolis, Maryland with her husband and two daughters, Alexandra and Georgia.

Senator CARDIN. Again, thank you for your testimony. Mr. Johansson.

**STATEMENT OF THE HONORABLE CHRISTIAN S. JOHANSSON, SECRETARY, DEPARTMENT OF BUSINESS AND ECONOMIC DEVELOPMENT, STATE OF MARYLAND**

Mr. JOHANSSON. Senator Cardin, Senator Mikulski, I greatly appreciate the opportunity to be here with you today at the Senate field hearing on Small Business and Entrepreneurship to really testify on the critical role that small businesses have and will continue to have in strengthening cybersecurity efforts in Maryland.

I want to thank both Senator Mikulski and Senator Cardin for standing sentry to protect our nation at home, abroad, and in the clouds, as well as your laser-like focus on our nation's economic recovery. On behalf of Governor O'Malley, I also want to acknowledge your steadfast support for Cyber Maryland, our strategic effort to make Maryland the epicenter for cybersecurity.

Let me also acknowledge Senator Mikulski's leadership in the Senate to create a National Center of Excellence at NIST, and we appreciate all of her efforts on that.

My testimony today will outline some of the steps that we are taking in Maryland to support and create jobs in cybersecurity and preview planned business development activities in the months ahead.

When President Obama first pledged to make securing the country's most vital computer networks a top economic and national security priority in 2009, he called for greater leadership and collaboration. Maryland answered that call with Cyber Maryland.

As Senator Mikulski outlined before, our State is uniquely positioned to seize upon this opportunity through our assets in Federal, private, and academic strengths, including, as the Senator mentioned, U.S. Cyber Command, a National Security Agency, the National Institutes of Standards and Technology, and numerous military commands, including a renowned academic institution producing the next generation of innovators and inventors, a broad base of entrepreneurs, and established businesses and intellectual capital second to none.

My agency engages stakeholders in Maryland's cybersecurity community to quantify and qualify the strengths of our state, identify business opportunities, and outline a strategic plan to capitalize on both. The results were unveiled 18 months ago by Governor O'Malley at NIST when Senators Mikulski and Cardin joined Dr. Gallagher and hundreds of business, academic, and federal leaders to launch this business development initiative.

Additionally, with Delegate Susan Lee's vision and leadership, legislation was passed during the 2011 session to create the Commission on Maryland Cybersecurity Innovation and Excellence. Our strategic plan included ten major action steps and was organized around four key goals.

First, support the creation and growth of innovative cybersecurity technology in Maryland. Second, develop an educational pipeline to train new cybersecurity talent and an advanced workforce development program like those being pioneered by institutions like UMUC, whom you will hear from shortly.

Third, advance cybersecurity policies to position Maryland for enhanced national leadership. And lastly, ensure the sustained growth and future competitiveness in Maryland's cybersecurity industry. I am pleased to report to you today that by the steps we have taken in government, and with the private and academic sectors, are successfully moving Maryland forward and positioning the state for Federal leadership in business, workforce, technology, and economic development.

In the interest of time and on behalf of my colleagues and other state agencies, I will touch upon three business development strategies we have successfully organized. The first one. We unified cybersecurity marketing under the Cyber Maryland brand to position our collective identity and enhance communication of the state's assets.

To date, a uniform logo, comprehensive website, and an aggressive social marketing campaign have been launched. You might see the logo here that we have created. I have got a slide here for the Website that you can access as well.

Next week, the Cyber Pulse will also debut that will communicate news about this growing IT sector. And you are seeing it before anybody else. In the coming months, we will launch a new strategic advertising campaign and target the markets and participate in a comprehensive outreach program of industry-based trade shows and conferences.

Second, we have positioned new start-ups for growth for capital funding by passing Invest Maryland in the 2011 legislative session to recapitalize the Maryland Venture Fund. And, Senator Cardin, also thank you to you for your leadership on the Senate Banking Committee when Congress passed the Small Business Credit Initiative. This is resulting in $23 million that is going to help Maryland's small emerging and minority companies secure access to credit.

Both of these programs offer significant opportunities for cybersecurity companies, particularly, and software communications and IT security. For example, the Maryland Venture Fund has already invested in there cybersecurity companies, Tenable Security, Sourcefire, and Oculis Labs. We believe there are opportunities for further cybersecurity investments that are going to grow exponentially.

With the federal and state tools, DBED will target early stage companies and products and collaborate with our partners to find vet and co-invest in early stage cybersecurity companies. These investments will be 50,000 to 250,000.

Three, we have made real progress on academic workforce programs to teach, train, and attract talent. For example, the Department of Labor Licensing and Regulation created the pathways to Cybersecurity Careers Consortium, a three-year program to train 1,000 workers to fill cybersecurity jobs in Maryland. With the support of Senators Mikulski and Cardin, we received nearly $5 million in U.S. Department of Labor community-based job training grant funding.

The Maryland Higher Education Commission provided BRAC higher education fund grants to community colleges, colleges and universities to develop cybersecurity curriculum. The University of

Maryland College Park brought together all cyber-related disciplines in the new Cyber Center, MC2, which is focused on cyber education, research, and testing.

These initiatives and others, like the Governor's Workforce Investments Board and Cybersecurity Subcommittee, are preparing students, retraining employees, and fueling a pipeline of cyber warriors.

In conclusion, cybersecurity offers business tremendous opportunities for collaboration with our universities; our incubators, including Chesapeake Innovation Center, the first dedicated to homeland and national security; our tech councils; our military commands; our Federal agencies.

Cybersecurity offers entrepreneurs and innovators of the prospect of discovery, detection, and defense to protect our nation's digital infrastructure and our State tools, talents, and technologies to lift our economies. Cybersecurity offers Maryland the potential to protect the nation's digital infrastructure, to attract and expand Maryland businesses to provide jobs for our highly skilled and well-educated workforce, and to benefit all regions of the State.

We see the innovation and job creation prospect of cybersecurity every day in entrepreneurs like Eric Fiterman, a former FBI special agent who founded Rogue Networks to provide protection to government Internet, protection to government and business clients, and Karl Gumtow who founded CyberPoint, and in just 18 months, created almost 100 jobs in Baltimore City.

We thank you for your support of these efforts.

[The prepared statement of Mr. Johansson follows:]


Testimony of

**Christian S. Johansson**

*Secretary*

*Maryland Department of Business and Economic Development*

*401 East Pratt Street, Baltimore, Maryland 21202*

*Before the*

**Committee on Small Business & Entrepreneurship**

**United States Senate**

**The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States**

*July 25, 2011*

*On behalf of*

*Maryland Department of Business and Economic Development*

*The Department's mission is to create, attract and retain jobs and promote Maryland's vibrant culture, heritage and arts.*

## I. Introduction

Chairwoman Landrieu, Ranking Member Snowe, Senator Cardin, and Members of the Committee, thank you for the opportunity to appear before you today to discuss the importance of cybersecurity to the United States and the role of Maryland businesses in this critical endeavor.

I am Christian S. Johansson, Secretary of the Maryland Department of Business and Economic Development (DBED). As part of the *CyberMaryland* Initiative launched by Governor O'Malley 18 months ago, we are helping a myriad of companies – start-ups, veteran-owned, minority-owned, and established businesses – put their talent, their innovations and their expertise to work to safeguard and secure our nation's digital infrastructure.

Senator Cardin has been steadfast in his support of *CyberMaryland* and of the businesses engaged in cybersecurity efforts, not only here in Maryland but across the U.S. Both Senator Landrieu and Senator Snowe have been champions of the small business community and our state is very grateful for their dedication and hard work.

## II. Acknowledgements

I would like to thank Dr. Patrick Gallagher of NIST, Jennifer Walsmith of the National Security Agency, Dr. Charles Iheagwara of Unatek, Inc. (recently recognized as Maryland's Homeland Security Company of the Year), Sarah Djamshidi of the Chesapeake Innovation Center, and Dr. Gregory von Lehmen of the University of Maryland University College. It's a privilege to testify with such prominent and respected leaders.

I also want to acknowledge Governor Martin O'Malley, who has embraced the challenge of keeping our nation and our data secure – not only as Governor of Maryland, but also as Chairman of the Democratic Governors Association and Co-Chair of the National Governors Association's (NGA) Special Committee on Homeland Security & Public Safety.

## III. Purpose of Testimony

My testimony today will highlight state programs and the ways in which we support small businesses in the cybersecurity arena. I will also discuss cyber-related contracting opportunities available to small, minority and veteran-owned businesses. The CyberMaryland Initiative has qualified Maryland's cybersecurity strengths, identified opportunities and outlined a strategic plan to capitalize on both.

### *CyberMaryland* Background

### Introduction

In 2009, President Barack Obama pledged to make securing the country's vital computer networks a top economic and national security priority. In doing so, he called for greater leadership and collaboration to improve the safety of information networks that power the

government and the U.S. economy. Maryland – with its vast resources of federal facilities, academic institutions, industry strengths and intellectual capital – answered the call.

Governor Martin O'Malley charged DBED with cataloging the state's information security assets and developing a comprehensive strategic plan to expand and enhance business and job opportunities in the fast growing field of cybersecurity. DBED interviewed 50 Maryland cybersecurity stakeholders to assess how best to participate in national cybersecurity activities while simultaneously developing a vibrant industry to create new jobs, drive sustained growth and generate innovations for the benefit of our nation and our state. Through this analysis, DBED identified key assets that could be leveraged as catalysts for short- and long-term growth of the state's cybersecurity industry and developed policy recommendations and actions.

Governor O'Malley released *CyberMaryland: Epicenter for Information Security & Innovation* and announced the Initiative in January 2010 at the *CyberMaryland* Summit, held at NIST. The report was recognized by the Council for Community Economic Research with their 2010 Excellence in Research award.

**Four Pillars**

The four priorities identified in the *CyberMaryland* report included:

- Support the creation and growth of innovative cybersecurity technologies in Maryland.
- Develop an educational pipeline to train new cybersecurity talent and advance workforce development.
- Advance cybersecurity policies to position Maryland for enhanced national leadership.
- Ensure the sustained growth and future competitiveness of Maryland's cybersecurity industry.

**Implementation**

Since the *CyberMaryland* launch, hundreds of thousands of people have learned directly about Maryland's cybersecurity expertise, assets and workforce through presentations, trade shows, conferences, and an aggressive proactive multi-media communications strategy. The *CyberMaryland* report and the increasing importance of cyber innovation to government, education and the commercial market have spurred an exciting range of initiatives in state government, and among various institutions and businesses, public and private. These initiatives span workforce and education, marketing and business development, commercialization and financial investments. Some of these are highlighted below.

## IV. *CyberMaryland* Moving Forward: A Business Development Priority

### 1. Brand & Unify Maryland's Dynamic Cybersecurity Market Sectors with Innovation

Developed Phase I of the *CyberMaryland* brand marketing program; launched new website (CyberMaryland.org), electronic newsletter and social media marketing campaign. Phase II will unveil a new, market segment targeted on-line and geographic advertising campaign and trade show participation and outreach.

### 2. Targeted Business Development: Expand and Attract Companies, Capital & Talent

**Conferences, Symposia and Trade Shows**

Maryland's strengths in cybersecurity have enabled three major industry-related conferences to be held in the state, most notably the C4ISR Joint Symposium and Expo at the Baltimore Convention Center in August of 2010. DBED has actively participated in these and other such events around the country. An extensive trade show participation plan is underway and a new exhibition will debut in August at MilCom and nationally at RSA in February 2012.

## V. Federal Opportunities and Small Business

**Team Maryland Network**

In 2010, the Federal Facilities Advisory Board created the Team Maryland Network, compromising nearly 140 members representing small, medium and large companies conducting business with the federal government. The Network's mission is to increase federal procurement expenditures with Maryland businesses and to foster cooperation among Maryland-based companies pursuing federal contracts. Over 50 business leaders and sub-contractors participated in the first Team-Up Maryland event in May 2011, including representatives from Lockheed Martin, Northrop Grumman, Booz Allen Hamilton, CSC, ARINC, LMI, L-3, Raytheon and SAIC. About 75% of the members are from the IT, communications or cyber sectors.

**Contract Connections**

Contract Connections is a series of conferences and forums on federal government contracting that DBED conducted that also help small and minority firms directly connect with large contractors doing business with the federal government. Both events filled up quickly and a third event is scheduled for December 2011.

1. Contract Connections Inaugural Conference, December 2010 – 13 federal agencies presented their contracting opportunities to 220 attendees. Over 300 matchmaking sessions with 13 agencies.

2. Contract Connections for Women, April 2011 – offered a targeted seminar on new SBA program for enhanced contracting opportunities for Women–Owned Small Businesses. Several agencies and a prime contractor presented business opportunities to 140 attendees.

## VI. Commercialization and Capital: Position Cyber Companies for Growth and Capital Infusion

### Seed and Venture Capital

There are a growing number of angel and venture capital fund investors exploring the diverse cyber industry, and they are investing in promising companies. Seed and early stage investing remains challenging, and we continue to play a supporting role in capitalizing and nurturing emerging firms in Maryland.

The Maryland Venture Fund (MVF) is a state-funded seed and early-stage equity fund that makes direct investments in technology and other companies. The Fund typically co-invests with private investors. Approximately 60 percent of the Fund is invested in technology companies in the areas of software, communications, and IT security. Past cybersecurity investments include:

- **Sourcefire:** World leader in intelligent cybersecurity solutions with Real-time Network Awareness and Real-time Adaptive Security solutions. Named to Forbes List of America's 25 Fastest-growing Tech Companies, the number one fastest growing cybersecurity on the list in 2011, this publicly-held Columbia-based company now employs 350+, 250+ in Maryland with $130M+ sales revenues.
- **Tenable Security:** Leader in Unified Security Monitoring. This privately held company has 100+ employees and is located in Columbia, Md.
- **Oculis Labs:** Developing data privacy software that secures the data between the user and monitor, this privately held company is based in Hunt Valley, Md., and has five employees.

InvestMaryland, an initiative passed during the last state legislative session, will raise $70M in capital that will allow Maryland to significantly expand the Maryland Venture Fund and target equity capital to selected venture capital firms investing in Maryland. Through this very important mechanism, we will be able to substantively make an impact on small and start-up cyber businesses. Funds will be available in spring/summer 2012.

The funding Maryland received from the Small Business Credit Initiative has made it possible to accelerate our cyber capital focus currently, as up to $7 million is allocated to the Maryland Venture Fund. Combined with the more than one million dollars in capital available in this fund, DBED will target early-stage companies and products and collaborate with our partners to find, vet and co-invest in early-stage cybersecurity companies. These investments will be in the $50,000 to $250,000 range.

These initiatives will require developing a pipeline of viable companies needing equity to grow, and we are working with public and private sector partners to find, vet and prepare potential candidate companies. As one example, we will partner with TEDCO to organize cyber-focused speed pitches, bringing potential investors and start-up firms together.

## VII. Workforce and Higher Education: Teach, Train and Attract Talent

### Cybersecurity Careers Consortium

The Maryland Department of Labor, Licensing and Regulation created the *Pathways to Cybersecurity Careers Consortium* to train future cyber workers. This three-year program will train future cyber workers for the estimated thousands of new technical jobs expected to grow in the I-95 corridor. For example, the Anne Arundel County Workforce Development Corporation received $4.9 million to train workers. By the time the program ends in 2013, as many as 1,000 individuals will have enrolled.

### Maryland Higher Education Commission (MHEC)

DBED worked with MHEC to organize the MHEC Internship Information Center website for cybersecurity and BRAC-related internships and job postings. MHEC also issues the online *CyberEd News* with links to affiliated State and education sites.

### Cybersecurity Task Force Report

The University System of Maryland established a Cybersecurity Task Force in November 2010 to inventory and assess cyber-related curricula; DBED staff was actively involved in this analysis. Released in May 2011, the report recommended and reinforced commercialization strategies and tech transfer investments.

### Industry and Higher Education Consortium

DBED and its academic partners would like to dedicate part-time staff to organize, coordinate and prepare for an industry and higher education consortium, across private and public institutional spectrum. This is already happening on a smaller scale at UMBC and UMCP.

## VIII. Cyber Commission: Educate Public and Legislature about Cyber

### Commission on Maryland Cybersecurity Innovation & Excellence (SB557/HB665)

With the leadership of Delegate Susan Lee, the Maryland State Legislature established Commission on Maryland Cybersecurity Innovation & Excellence that will include state and local networks. The focus of the Commission is to undertake a comprehensive review of the cybersecurity needs of the state and will include securing state and local networks.

### Public Education and Awareness

Under the leadership of the Maryland Department of Information Technology, the state developed an initiative to educate citizens and small businesses about cybersecurity. As part of the national cybersecurity awareness month in October, the state conducted local awareness campaigns. High-profile activities are planned for this October, notably the **Maryland Cyber Challenge and Conference (MDC3).** DBED has joined SAIC, UMBC, the Tech Council of Maryland and the National Cyber Security Alliance (NCSA) to host this inaugural event to convene the best cybersecurity minds among Maryland's students, academia and professionals.

## IX. Conclusion

Threats in cyber space now impact every facet of every system that supports the world's connected and collective infrastructure: commerce, public safety, transportation, finance, energy and health are all driven by and require safe, secure and strong systems. As the epicenter for cybersecurity information and innovation, Maryland is committed to improving the networks that power the U.S. economy.

We will continue to support the education and development of a qualified workforce, able to meet the challenges of today and tomorrow through the creation and provision of training curriculum and programs in all our educational institutions. We will continue to build sensitivity and awareness among our citizens through public education and outreach on protecting professional and personal networks. We will support our small and medium-sized companies in every way we can so the future technologies will support and protect our critical infrastructure, networks and information developed and brought to market from Maryland.

Cybersecurity companies have emerged as centers of innovation, creativity and job creation and we will continue to invest in them. Finally, as a state that has the privileged position of being home to unique federal and military institutions charged with protecting this country, we will continue to provide strong advocacy and a supportive business environment.




**Christian S. Johansson**

Secretary Christian S. Johansson leads the Maryland Department of Business and Economic Development with an accomplished background in economic development, management consulting, technology and healthcare.

Mr. Johansson has spearheaded many state and federal initiatives since he was appointed by Governor Martin O'Malley in April 2009. Under his leadership, the Department re-launched the Maryland Economic Development Commission, and helped create and execute the Federal Facilities Advisory Board, International Advisory Council, and the Governor's Commission on Small Business. Other initiatives include helping to craft federal legislation for a $1.5 billion credit provision to the Small Business Jobs Act to expand small business loan guarantee programs nationwide, and *Invest*Maryland, an administrative and legislative initiative aimed at creating a public-private partnership to fuel venture capital investment.

Before joining the Agency, Mr. Johansson had a brief role as Managing Director with Continental Equity. Prior to Continental Equity, he served for six years as the CEO of the Economic Alliance of Greater Baltimore. When he was selected at age 31, he was one of the youngest in the nation to run a top 20 regional economic development organization. Before joining the Economic Alliance, while in Boston, Mr. Johansson was Senior Consultant for the Sag Harbor Group. In 1999, he founded and served as CEO of Inka.net, a venture-backed CRM enterprise software company. In 1995, he founded Dola Health Systems, a medical assessment and consulting company which had operations in Baltimore and Stockholm, Sweden.

Mr. Johansson earned a BS in Biology from Brown University and a Masters of Business Administration from Harvard University. He was named one of the *Baltimore Business Journal's* "40-Under-40" emerging leaders and was recognized by *Leaders Magazine* as one of seven Central Maryland executives. In 2010, Mr. Johansson was recognized as an Innovator of the Year by *The Daily Record* for having "a positive effect and tremendous impact in Maryland" and a Special Advocate at the Top 100 Minority Business Enterprise Awards. Secretary Johansson serves on numerous boards, including the Carson Scholars Fund, the Governor's Subcabinet for International Affairs, the Maryland Economic Development Commission, Federal Facilities Advisory Board and many others specified in the Maryland Manual. He also served on President Obama's transition team and Executive Committee for Urban and Metropolitan Policy.

Senator CARDIN. Well, thank you all for your testimony. Secretary Johansson, let me first compliment the O'Malley Administration. The purpose of this hearing is to put a focus on cybersecurity and the role of small businesses, and I think under the leadership of Governor O'Malley, we have seen a Governor who has taken the advantages we have in Maryland through the Federal facilities that are there, the colleges and universities, and then put it together with the interest of the Governor, support of the Governor, to really provide the impetus for significant movement in our State with economic growth.

We are here to talk about small businesses and you said something during your testimony I want you to talk a little bit more about. Part of the legislation we passed for the small business community was the deal with the availability of credit, which is one of the major concerns. Small businesses do not have deep pockets, and during these tough economic times, it is hard to get loans.

So we made an extraordinary commitment of additional Federal resources. It was, quite frankly, all going to be managed at the national level through direct support to community banks. Then a Governor named O'Malley petitioned the Government to say, Look, the States can leverage a lot of this money. Give us part of those funds.

And a very small part of those funds were allocated to the States as a result of the efforts of Governor O'Malley and other Governors, with the commitment that those funds would get out to help small businesses.

We recently had a briefing from the SBA as to what was happening with the Federal portion. I must tell you, there was bipartisan concern the money was not getting out fast enough, that we needed to get it out quicker. And we are talking about $30 billion, a lot of money that could be leveraged.

You mentioned in your testimony about three companies. Can you just tell us how the Governor has used these resources to try to get money out to small businesses, particularly in the cybersecurity area?

Mr. JOHANSSON. Sure. Here we go. First off, there was an application that all the States needed to complete. I believe Maryland was the third State in the union—maybe was the fourth State in the union to complete it and receive funds which we recently did. We are receiving $23 million. Out of that $23 million, we intend to split it between different pools.

Now, one pool will be going into our MIDFA program which helps guarantee small business loans. About $7 million, however, is going to our Maryland Venture Fund. Almost half of the opportunities that we have traditionally invested in have been technology opportunities, many of them in cybersecurity, and I just listed three examples of companies that we have invested in, in the past.

Senator, I really thank you for your support of this because what this effectively means is, as a result of this, there is $7 million, and if history is any guide, probably about half of that is going to be invested directly into some of the more emerging, pioneering, small businesses here in Maryland that need equity capital to grow and to expand.

Senator CARDIN. If you could make that information available to our Committee, we would appreciate it very much for our record, because I think it would be helpful to share that with the other members of the Senate to show that we are getting the money out faster through the States and leveraging it for more economic activities. So it would be good to have the specific examples.

Mr. JOHANSSON. We will get you that, Senator.

Senator CARDIN. Director Gallagher, you mentioned a very important point about cloud computing, and when you think about it, if you are a small tech company, you are trying to compete, computer capacity is one area that is going to be raised by the contractor as to the capacity versus the large, traditional prime contractors that you normally selected.

Can you just talk a little bit more about how you are working on cloud computing so that it does somewhat equalize the capacity of being able to use computer technologies for a small company that is using innovation and technology?

Dr. GALLAGHER. Yes, thank you. I think that one way to think about the cloud model is it is an approach that turns IT resources from a built-in, capital-intensive enterprise that you need to build out within your company and turns it, frankly, into a commodity that you can purchase and scale up very quickly.

So it is a great equalizer. In fact, I think it is poised to continue to make information technology even more of a commercial advantage than it has already proven to be. If you can imagine, the ability now to set up eCommerce sites, Web sites, and business systems through cloud services rather than having to build those servers and build that infrastructure within your own company and have the capacity inside to manage it, you can begin to see some of the tremendous advantage that it allows.

It also is one of the few approaches that can rapidly scale. So if your company is really growing, if you are attached to your enterprise hardware, it is very difficult to keep up with the growth rate, perhaps, of a company. Whereas, through the cloud you can provision new resources almost immediately and scale very quickly.

And I think that the business community faces the same challenges in the cloud that the Federal Government does, which is it is still a new area. These different cloud-type services do not work well together yet, and so we have concerns about making sure if you move something important in your business to the cloud, you do not have a proprietary lock-in. You have got the flexibility in the future to move your data and your services to somebody else so that the market works.

You want to make sure the data that you put out in the cloud is secure. You want to make sure that the privacy of your customers is protected. And you want to make sure that it is available and reliable. And the fact that somebody else is now doing these things for you instead of you doing it yourself has changed the nature of the relationships.

So we are working very closely with the business community to try to come up with that sort of collective behavior and those standards to drive that forward. And I have to say, the small business community plays two very important roles.

One, they are going to be uniquely enabled by this infrastructure, but a lot of the innovation that Christian was talking about that is going to provide these solutions is going to come from that community as well. Their agility and their innovative capacity is going to play a key role, and we already see that in the NIST cloud efforts that the small business community are very active participants in this early effort.

Senator CARDIN. It is very exciting. I think NIST has a unique opportunity here, particularly as it relates to the portability and security and being able to make sure that you do not lose the proprietary information, which is one of the main problems for small businesses today. So I think it is extremely exciting, what you are doing there.

Ms. Walsmith, I want to ask you a question about your problems in meeting goals on prime contracting. I know you have made tremendous efforts: 17 percent is a good number, but 25 percent was the goal. So what are the challenges that you are confronting in getting more prime contract work to small companies under NSA?

Ms. WALSMITH. So we recognize that the goal is very critical that we meet. Some of our challenges are actually successes for the companies of which we do business with, and that is, often when we establish a relationship with an innovative small company, the first thing that happens, sometimes before I have even awarded the contract, they have been bought by a large company.

And so, that is a positive in terms of the overall aspect of what we try to promote in the American economy. On the other hand, as soon as a small business is bought, then I no longer can take credit for that small business opportunity.

But other things that we have to address, I do not want to say that it is that alone, is the growth of the small, small businesses. They do not always get represented in the first year. So let me explain a little bit further. So as we reach out to these really new tech innovative companies, generally it starts with a small dollar amount and then it grows over time.

So you do not immediately see the benefit in literal dollar amounts, but it is the number of companies that we are doing business with that really creates that pipeline in the seed corn of the growth that we see in the long term. So that is another important facet that you do not always see directly in the number itself.

The third area is to the challenges of just making those connections with the small businesses. It is a challenge for us to create enough time and opportunity for them to share their capabilities with us and for us to get to know them. That is where we have strengthened and grown our PISA program that I referred to earlier, our Provisional Industrial Security Accreditation Program, putting more in that pipeline this year than we have in any other year.

So this year alone we have put another 153 businesses into that, clearing them and their technical representatives in advance of any contract. Statistically, over 50 percent of those companies that are participating in PISA do result in a prime contract or business with us and within three years.

And so, those are the challenges that we face. We continue to push that further. We are very conscious of the large contracts and

one that we need to take the time to do those small business set-asides. And so, I myself, as well as all of my leadership team within the Acquisition Directorate, have performance goals specifically within our performance reports that speak to having to meet and achieve those small business goals.

But I would like to say one for a moment, it is not just about the numbers. It is really about our success. It is the thing that we need to be successful as an agency, so we do focus very much on bringing our numbers to the levels that you want and expect us to deliver against, but it is also about building that pipeline and the small set of businesses that we know are critical to our future success.

Senator CARDIN. Thank you. Senator Mikulski.

Senator MIKULSKI. Senator Cardin, this is just a great, great hearing. I would like to go first to you, Dr. Gallagher. Senator Cardin, first of all, you know what a great asset NIST is. I mean, it is the agency that sets the standards for all private sector—anything that is a proprietary product, that is invented and sold in the United States of America, the standards are developed there.

You would be interested to know that their total annual budget—under what I want to do, and what they consider adequate—is $1 billion. For $1 billion, we get a couple thousand people working in Gaithersburg, but also through what they do, we have millions of people working in the United States of America.

You would also be interested to know that the House Appropriations Committee has reduced Dr. Gallagher's appropriation to $700 million. They just think they are government, they are just so expensive, let the private sector do it. The private sector does not institute standards. They cannot institute standards. [The private sector] develops products that have to have standards, so they can sell it here and around the world. Seven hundred million dollars, which I think will have a big effect. This is not an appropriations hearing by proxy, but when people talk about "big government" and how we are going to make it smaller, by making this Government smaller—we are going to make the private sector opportunities smaller. Government and the private sector cannot do this.

Now, let us go to Dr. Gallagher. I wanted to, in last year's appropriation, put in $10 million for a National Cyber Center of Excellence to do tech transfer and some other things. Could you elaborate on what we wanted to do together? You have to know, in that awful CR shutdown situation that we went through, over which I am still prickly from that, let alone what we are facing now . . . so tell me what you thought it would do and what opportunities you think we have missed out on, or do we really need it? I am fighting, Senator Cardin, we are fighting for every nickel right this minute.

Dr. GALLAGHER. Thank you. I have to say, I am tremendously excited about the idea of the Cyber Security Center of Excellence, and the reason for that touches on the point you just made about NIST being drawn very broadly and having to cover a lot of area. That is certainly true.

The only way we have been able to preserve our effectiveness is to leverage what the American private sector can provide. It is really only in working in partnership with industry that we can even begin to approach some of these technology challenges.

And the truth of the matter is that the innovation of the new technologies, whether they are going to be to solve identity management, whether it is to solve the use of the cloud, whether it is to solve cybersecurity, happens at this mixing zone between what the Government is doing and what the private sector is doing.

Senator MIKULSKI. A mixing zone?

Dr. GALLAGHER. A mixing zone.

Senator MIKULSKI. Is that not a great phrase?

Dr. GALLAGHER. And the President has been very vocal about this idea of creating economic opportunity by solving the country's core problems, whether it is looking at energy technologies or what have you, we can simultaneously create new opportunities when we focus on a key challenge. I think cybersecurity fits in that arena.

By solving this big challenge, we are also opening up big opportunities for our businesses. And the concern we have had is, how do you provide an efficient forum for Government researchers and staff to work with basically, and that is really what the Cyber Security Center of Excellence was going to provide.

It is a place where those two communities get together and work on shared problems. It is a place where the Government can benefit from the innovations and new ideas that are there in the private sector, and it is a place where the private sector can benefit from some of the research results that are coming out from the university.

So it is almost more than tech transfer because we have information moving both ways, and I think a strong opportunity creates a mutual benefit for everybody. So we are continuing to work forward as much as we can with planning. We have been talking to our partners in the State. We have been talking with our partners in our other agencies to see how we can make this center create a focal point for business to work with the Government on these types of shared challenges.

Senator MIKULSKI. Well, I am going to continue to fight for you because that is really fighting for our—quite frankly, fighting for our jobs for both tech transfer and for NIST to be NIST. And in the world of the cyber domain, I think, Ms. Walsmith, if General Alexander were here, he would say, "Our weakest link is our strongest link."

In other words, wherever we are the weakest—and if small business does not protect itself, because we forget that some of the biggest bad guys against us are not foreign nationals, but organized crime, and they are going after small business in the identity theft area. So that is a hallmark. We could go on all day with you, and we look forward to working with you.

But, Ms. Walsmith, I would like to go to you. First of all, what a great pamphlet. Is this the one that you give out anywhere and anywhere?

Ms. WALSMITH. Yes.

Senator MIKULSKI. Now, if you could, Senator Cardin has already asked a couple other questions, but first of all, if you are a small business in Maryland, and I am thinking of the National Security Agency, do you give out—does NSA give out contracts to non-geek, non-security clearance agencies? Because many businesses do not even come to you because they think they have to be a geek com-

pany selling something in the world of signals and intelligence, and that they have to have a security clearance, which in and of itself can tie up a lot of capital in order to become certified.

So do you help? Are there opportunities for the non-geek companies, and what would they be where you do not need a security clearance, or maybe you do?

Ms. WALSMITH. So that is frequently a myth about the National Security Agency, is that all our work is classified. But, in fact, nearly 40 percent of our work is unclassified, and that is something that most people do not realize. That business range to support an enterprise worldwide ranges from the guard dogs to the fences to snow removal to IT servers to more traditional, high-end cryptanalytic capability.

But my point is that it crosses the spectrum of anything that you would need to run a large corporation worldwide. So we, in fact, have tremendous opportunities for businesses that are the non-technical organizations. In fact, when we look at our installation and logistics organization, if I looked at the statistics last month, over—let us see—of their appropriated budget, with the exception of the MilCon, they averaged around 58 percent of their appropriated funds goes to small business awards.

And so, there is tremendous opportunity for companies, other than those technology companies, to do business with us.

Senator MIKULSKI. So as we troubadour these opportunities, we can essentially say to small business, Anything you do to support any large enterprise—it could be security at a community college—you could also look at agencies that are literally teaching lessons around the world to bad guys, so they should come to you.

Now, walk me through. If you wanted to get started at the National Security Agency, what would you come to and where would you get started?—

Ms. WALSMITH. So the first thing——

Senator MIKULSKI [continuing]. To get beyond the fence.

Ms. WALSMITH. So the first thing we would say is to come to one of our biweekly sessions that talks to you about how to do business with NSA. That is what I referred to that we had sent hundreds, literally thousands of companies through that process where we sit down and talk to you about the first steps of doing business with us.

Senator MIKULSKI. So is that the gateway?

Ms. WALSMITH. That is the gateway. That is now housed within our fence line. It is actually at a location in Hanover, Maryland that does not have the——

Senator MIKULSKI. So it is actually a disclosed location?

Ms. WALSMITH. It is a disclosed location, though I will be careful in that—but it is a location that you can come to and not have to go through the normal process coming inside.

The second step is to register actually with our Acquisition Resource Center as we said. It is actually a mechanism to register companies and able to——

Senator MIKULSKI. And that is the ARC?

Ms. WALSMITH. That is the ARC. So those are your first two steps. From that, that then puts you in the availability pool for us to—when we send out a market survey, if your key word, your

business that you submitted, what capabilities you had, triggers that match within the database, then market surveys are automatically sent to you to provide you information on opportunities to do business with us.

We further move on to do one-on-one capability discussions. So there certainly are those that need a security clearance, and so we then host those one-on-one capability discussions, and sometimes that will result in us sponsoring someone into the PISA program. That is another avenue for them to come and do business with us.

We always host at least once annually, a forum which is specifically to unclassified companies to understand what it is like in terms of what it would take to get a clearance, how to do business with us, what is the ARC, what is the security process. And so, we are always trying to make it attainable.

Senator MIKULSKI. We would like to know the date of the next one because offering the entire delegation on a bipartisan basis—I know Congressman Bartlett is keenly interested in this. I am not sure about Congressman Harris, but I know Bartlett really is. He is an inventor, a patent guy, and has Fort Detrick. We would like to know that.

But your point to me is that each step leads to the next step, and so the gateway is at the Acquisition Resource Center and those first two biweekly meetings.

Ms. WALSMITH. Right.

Senator MIKULSKI. You come to those and you get underway. Is that correct?

Ms. WALSMITH. Yes, that is correct.

Senator MIKULSKI. Well, I would just like to say, Congressman—I have got the delegation on my mind now. Team Maryland. Mr. Johansson, again, we would like to thank Governor O'Malley for his leadership in making cybersecurity a top economic development issue. Again, safer country, stronger economy, and we all have to be smarter in how we do things.

I think Senator Cardin covered my questions to you, but we would like to compliment you on your work, and let us keep the path going. I know Senator Cardin and I are going to have to go to the Capitol, so again, I could have 5,000 more questions for 10,000 more small businesses, but I am going to stop because we are trying to avoid, literally, the collapse of our economy. So I think I have covered it.

Senator CARDIN. Well, let me thank Senator Mikulski again for being here. I know that she is going to have to leave shortly and I appreciate her joining the Committee for this period of time, and, of course, we appreciate her strong leadership in our delegation, to focus all of our resources of our delegation to support what the three of you are doing.

I have one last question which has to do with SBIR that we were unable to get off the floor of the Senate, but we will come back to it. My question to you, Dr. Gallagher and Ms. Walsmith, is, the goal, 2.5 percent, how you all are doing in meeting that. This would increase it to 3.5 percent set aside for innovative funds to small businesses. Are you meeting those goals? Do we need to do something different than was in the reauthorization bill?

Dr. GALLAGHER. So you are talking about the targets for the SBIR collection rate?

Senator CARDIN. Correct.

Dr. GALLAGHER. So for NIST, we tend to meet those targets fairly readily. We are not a large grant-making organization so our SBIR program is fairly modest by comparison. But we have been fortunate to not having any difficulty meeting those requirements.

Senator CARDIN. NSA, are you involved in this?

Ms. WALSMITH. So we participate through DOD and we do very well with the SBIR program, but we are participating in through the DOD process.

Senator CARDIN. I thank you for that. One last point, Ms. Walsmith. Your point about the contract officers and reaching out to small businesses, you made a very good point about the smaller company being bought out by the larger company, which many times is exactly what they want to happen. Sometimes they have to do it by necessity because they need to be into a larger enterprise. That may not always be the best, but in most cases, it is.

Just very quickly, does the current budget problems put an extra burden on your contract officers or directors as to whether they have the resources to be able to look beyond their current set of contractors?

Ms. WALSMITH. So certainly as we have been—the challenges this year with the continuing resolution and what it then results in for us executing our budget in very distinct increments puts an additional workload on our contracting officers. That does draw attention away from the outreach to bring in new businesses.

We work to balance that very stridently to ensure that they are still spending the time, but the first thing that comes onto the plate is ensuring that we are appropriating the funds we have aggressively and to meet the needs that we submitted that budget for.

Senator CARDIN. Well, thank you. On behalf of Senator Mikulski and myself and the Committee, I want to thank all three of you for your time, for getting through the weather today. It started out just muggy and hot, then it just became wet and muggy. But we thank you very much and we look forward to working with all three of you.

We will now turn to Panel 2.

## PANEL 2

Senator MIKULSKI. Senator Cardin, I am going to have to go because of the situation and trying to organize the women of the Senate so we are not thrown under the bus.

Senator CARDIN. Again, I thank you.

Senator MIKULSKI. So if I could be excused?

Senator CARDIN. I think everybody knows the current situation on Capitol Hill where we have eight days to a deadline to make the August 2nd on the budget. Senator Mikulski is in the middle of some of those negotiations. When I leave here this afternoon, I will be going back to Washington to join in that debate. Quite frankly, it is more enjoyable being here with you all, but that will require me to go back to Washington this evening.

Let me welcome all three of our panelists on this panel. First let me welcome Dr. Charles Iheagwara who is the Chief Marketing and Business Development Officer at Unatek, a U.S. Government information technology contractor. He leads business development efforts with several notable successes, including positioning Unatek as a major U.S. Government prime contractor and expanding corporate business lines, contracting, and marketing services in the workforce.

He has also previously worked for the District of Columbia Government and a number of other companies including Lockheed Martin. Unatek recently received the Homeland Security Company of the Year award from the State of Maryland. Congratulations on that.

Next we will hear from Sarah Djamshidi. As the Executive Director, she oversees all of the Chesapeake Innovation Center's activities, coaches and mentors in the member companies. CIC is a unique venture accelerator that connects promising technology companies and emerging technologies with Government agencies, major government contractors, and private sector customers.

Last we will hear from Dr. Gregory von Lehmen, who serves as Provost and Chief Academic Officer for UMUC, University of Maryland, University College. He joined UMUC as the Area Director for Japan in 2001 and worked for UMUC Asia as Area Director for Japan for four years.

He returned to the United States in 2005 where he served as the Senior Associate Dean within the School of Undergraduate Studies and later as Senior Vice Provost. So with that, let me start first with Dr. Iheagwara and then we will move on to our other witnesses.

**STATEMENT OF CHARLES IHEAGWARA, Ph.D., CHIEF MARKETING AND BUSINESS DEVELOPMENT OFFICER, UNATEK, INC.**

Mr. IHEAGWARA. Thank you, Senator Cardin and members of the Committee for inviting me to testify on this very, very important topic, that is the Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States, and if I may, to a large extent, the cybersecurity portion of the entire planet.

As I stated in my written submission, my experience is one of ten years of both field practice and the academic work, and as you mentioned earlier, I worked with a couple of companies, including Edgar Online, Lockheed Martin, and the D.C. Government eight years.

On the academic side, also, I have been fortunate somehow to have written two topics on cybersecurity. My Ph.D. dissertation in Cardiff, Wales was on cybersecurity, and in particular, the effectiveness of intrusion detection systems. I also wrote a thesis recently at MIT on cybersecurity.

Having said that, Senator, I want to now focus—direct a few points that the role of small businesses play in strengthening cybersecurity in the United States. And in my written submission there are six key areas, one of which is talent, the second is capacity creation, the third is incubation, and the fourth is innovation, both of course of new technologies, processes, and practices. The

sixth obviously is providing new services that are not always readily available from the large firms.

Now, all of these are important for the reason that in seeking a solution to, of course, America's cybersecurity problems, it will be hard to think of any group closer to the action than small businesses. Small businesses in this case carry an extraordinary burden of leadership in both addressing the current threats and also, by the way, by way of their innovativeness, charting a course for developing cybersecurity to process these technologies, et cetera.

By most accounts, one would really agree that in times of job creation, the significant impact here is that small businesses overall add the net growth in all jobs created. For example, economists with the Kaufman Foundation have determined that companies that produce most jobs are the new ones and that since 1980, nearly all net job creation has come from companies less than five years old.

I do know this firsthand, having graduated recently from MIT, that this is true. The President of MIT, Susan Hockfield, stated—gave the statistics last week, and in the statistics she mentioned that each year MIT alone creates 900 companies a year. Well, if we go by the statistics readily available, 90 percent of them would fail. That means that 10 percent of them will succeed, and that is 90 companies each year singularly.

Now, when we multiply this by dozens of other schools, who alone launch small businesses, then obviously we have a multiplied effect here. That is very, very important. And why is this important to mention? It is very, very important to see small businesses not just as businesses that have been formed within the legal confine of what we typically call a corporate structure.

Yes, these small businesses are independent consultants. These small businesses have been graduate assistants who have been incorporated legally. Some were doing business with the government or the state. So it is very, very important to say that.

And by extension, the talent tool provided by small businesses is overwhelming, for the mere fact that small businesses are in the front line of solving problems, addressing security problems, and to a larger extent, in the growth economy, confronting also some of our problems. By certain, they are able to develop talents which are not readily available or acquired from the universities, so this is one significant area where small businesses contribute greatly to the economy.

We want to also state that capacity creation is one of the six main areas that small businesses are actively engaged in, in strengthening the cybersecurity of the nation. Many of the initiatives at the Federal and State levels spur, as we know, capacity creation. A case in point is the recent DFAR changes proposed by the DoD that will affect the entire DoD supply chain. This in itself is going to have a multiplier effect by creating different capabilities that will affect job creation, not just within small business establishments, but also for large businesses as well.

And, of course, we know that the most talked about efforts on incubation and innovation of technologies of two processes and all sorts of innovations come from small businesses. This is very, very correct. For example, in our own Maryland here, State of Mary-

land, Sourcefire, Inc. created the SNORT. The SNORT is one of the intrusion detection system tools that is out there today. It is assumed to be the informal baseline. It was created by a small business and has expanded today all over the world. Somehow the SNORT is used as the standard.

We also have, as Secretary Johansson mentioned, Tenable Security, a software company located also in Columbia, Maryland here. It is still the—the scanning tools, software scanning tools that it created also have set standards.

So we can go on mentioning countless small businesses throughout the United States of America that have come up with new technologies that have incubated them and that have innovated existing technologies or that have somehow incubated new ones outside the traditional confines of large institution-based or Government-based research and development labs. Very, very important.

And lastly, Senator, I will also submit that niche services is an area where we think small businesses have overwhelming governance. For example, in the field of cybersecurity, we do know that the hacking skill is very, very important in the fact that folks that have these skills are able to assist in what we call penetration testing.

We have often heard about the Tiger Teams, Red Teams, et cetera, that are called in from small consulting firms or consultancies to help big companies and Government agencies that test the health of the security devices that they have mounted or employed.

Such niche services are never incubated by large businesses, but small businesses provide them, and, of course, we have heard about the celebrated case by one of the famous hackers, Kevin Mitnick. He had great hacking skills and there are thousands of more like him today. So it is very, very important to say that niche services is an area where small businesses have overwhelming dominance.

But let me conclude my brief presentation by saying that these contributions by small businesses, there are enormous obstacles, as you have noted, and also Senator Barbara Mikulski. But I do want to suggest that it will be good for us to recognize that growing new ideas take money. Capitalization is very, very important.

We are aware of the fact that Congress has passed different legislation to help small businesses secure loans, but the banks are not lending. Recently my company, despite of our resources or in spite of our resources, I do not know which is best to describe here, approached a bank to get $200,000 in a loan and we were declined because we have maxed out, and we have a niche service that was tested that is very, very successful. So this is one of the challenges.

So one way that small businesses can actually capitalize fast is for them to get contracts as primes or subcontractors. We do note that the big companies are good at what they do, but, of course, it is also the fact that they are greedy. They go after $50 contracts head to head with small businesses.

So I think one of my first recommendations is that Congress probably should consider mandating a certain percentage of all Federal contracts to go to small businesses. Then secondly, I think in furtherance of the different loan programs out there, it might be good for also Congress to consider ways of granting low-interest

loans to support small business innovations such as I have described, the one of growing the company.

And also, we have heard that Cyber Maryland has an initiative that falls outside cybersecurity in the State, but it will also be good if small businesses are included in such initiatives both at the Federal and State level. Oftentimes the impression is that they are included, but obviously if you look around, you do not know who is included.

So, Senator Cardin, I want to thank you and the Committee for giving me the opportunity to testify here today, representing thousands of small businesses. I would be glad to answer your questions.

[The prepared statement of Mr. Iheagwara follows:]

**UNITED STATES SENATE**

**COMMITTEE ON SMALL BUSINESS AND ENTREPRENEURSHIP**

"The Role of Small Businesses in Strengthening Cyber Security Efforts in the United States."

**TESTIMONY OF Charles Iheagwara, Ph.D., CISSP, PE**

**Chief Marketing and Business Development Officer**

**Unatek, Inc.**

Monday, July 25, 2011

Good afternoon. Thank you, Senator Cardin, and members of the Committee for inviting me to testify today on issues pertaining to the role of small businesses in strengthening Cyber security efforts in the United States. Cyber security is a practice I have been engaged in for well-over 10 years now, has meant a great deal to my company, and I look forward to telling you a bit about my experience.

My experience in Cyber security spans different domain areas of practice with big and small firms and federal and state government consulting. As well, I have deep-rooted academic background on Cyber security having written a Ph.D degree Dissertation titled: "The Effectiveness of Intrusion Detection Systems" at the University of Glamorgan, Wales, UK and most recently an MS degree Thesis titled: "The Strategic Implications of the Current Internet Design for Cyber security" at the Massachusetts Institute of Technology (MIT), Cambridge, USA.

Since my professional practice started in January, 2000 as a security engineer at Edgar Online, Inc. (formerly known as Financial Insight Systems) that maintained a significant portion of the NASDAQ IT and technical infrastructure, I can truly say that every day has been a learning experience. Working collaboratively with lines of operations department unit heads and IT security personnel I gained valuable knowledge on the scope and depth of vulnerabilities and high risks that characterize Cyberspace and the essential elements of mitigation approaches.

Additional field experience was gained through my lead consulting roles at Lockheed Martin, KPMG and Aligned Strategies Development Corporation. Also at Unatek, Inc., I have led several client engagements and project implementations delivering Cyber security solutions to federal, state and local governments.

Unatek, Inc. as an Information Technology consulting firm has established a niche in Cyber security solutions and services. Although founded in 1996 as an environmental engineering company, it changed its business line in 1998 to Information Technology

and ever since then has provided Cyber security services to several federal and state government agencies and many public sector organizations. Most recently, Unatek, Inc. was the recipient of the 2011 "Maryland Homeland Security Company of the Year" award (http://thedailyrecord.com/2011/06/03/maryland-incubator-company-of-year-award-winners-named/).

In the last three years, Unatek expanded the scope and range of its Cyber security services and operations to include several niche services in Security Engineering and Architecture, Risk Management and Advisories, Continuous Monitoring, Computer Incident Response and Forensics Investigations, FISMA Compliance, Training, Security Operations to mention but a few.

Current and past clients include the US Department of Commerce, US Smithsonian, US Department of Labor, US Department of Veterans Affairs, US Marine Corps, US Department of Homeland Security and the District of Columbia government. Private sector clients include the Metropolitan Washington Airports Authority, Washington Metropolitan Area Transit Authority, Reagan National Airport, Dulles International Airport, KPMG and Lockheed Martin.

Branding of specialized unique products and services are under way in the company. In the last five years we have successfully incubated and branded a world-wide Cyber security conference and expo suites (http://www.unatekconference.com/intrusion_home.php) that provides the forum for security professionals to collaborate, exchange ideas and transfer knowledge. To date, three (3) events have been organized and plans are underway to make this a permanent feature of our practice. We are also in the process of incubating a Cyber security analyst and online media service that when fully developed, will provide analytic services on the technologies, products and processes that enable Cyber security and the marketplace dynamics that drive growth in the sector.

As a Cyber security company, we are a frontline problem-solver and are constantly at the forefront of technological advances, government policy, envisioning the need for information and operational security, investing in facilities, corporate infrastructure and personnel to expand our service offerings as a highly qualified Information Technology company. Unatek continues to be an early adapter of advanced processes, toolsets, security technologies, and services necessary to support our federal and commercial clients. This coupled with our dedication and commitment has ensured lasting relationships with our government and private clients over the years.

As a small business we have successfully executed on very complex Cyber security projects. For example, we provided niche subject matter expertise for Lockheed's next generation intrusion detection systems. As the Computer Emergency Response Coordinator, our staff directed intra-agency emergency technology for District of Columbia. At the Dulles International and Reagan National Airports, together with our KPMG partner, we provided risk management solutions that mitigated risks and enhanced security at two of our nation's busiest airports.

Leveraging the products and toolsets of our strategic business partners (Juniper Networks, Microsoft Corporation and Cisco Systems) we provided Business Intelligence training to the US Department of Veterans Affairs, multi- track certification training in various networking and security domains to the US Marine Corps in satisfaction of DoD 8570.1 Directives, and FISMA training to the US Department of Homeland Security.

At the US Department of Labor, we provided FISMA and complex Continuous Monitoring support; and Certification and Accreditation support to the US Department of Commerce and the US Smithsonian Institution.

Unatek is also providing very specialized niche Cyber security services to a variety of quasi-government and private sector clients. For example, Unatek is providing specialized PeopleSoft application security support in addition to network security support to the Washington Metropolitan Area Transit Authority. Also in the recent past, we set up a Cyber security lab and trained several Cyber security personnel at the medium-sized audit firm of Thompson, Cobbs, Bazilio and Associates (TCBA), and provided a wide range of consulting services to incubate and nurture their Cyber security practice.

The contributions made by Unatek in helping the nation combat Cyber attacks mirrors those made by countless other small businesses. As a small business, providing Cyber security solutions and services is not always easy due to a variety of reasons primary of which is the limited availability of resources to expand services and market. But, reliance on several factors such as low-overhead, resourcefulness of our personnel, availability of niche expertise within our talent pool, effective management of project execution and a very efficient alignment of corporate resources have been the key to our successes.

Like hundreds of other small businesses, we continue to partner with other business entities in the Cyber security field. We are reseller's of Cyber security products from big-sized businesses such as McAfee, Inc., Juniper Networks, Cisco Systems and small-sized firms such as TransGlobal Business System. We are also constantly pursuing teaming, subcontracting and other collaborative ventures with firms like SAIC, Booz Allen Hamilton (BAH) and others that rely, in no small measure, on small businesses to deliver services and solutions.

All over the country, there is growing evidence that small businesses are playing an important role in the US national and local economic development. SBA data demonstrate that small businesses provide majority of new jobs and produce much of the creativity and innovation that fuels economic progress. On this, Unatek has provided employment to many and every new contract means new employment and additional source of revenue to support growth and expansion of services.

In the national economy, small businesses are the employees, the customers and the suppliers who provide goods and services to the federal, state and local Cyber security markets. They also provide significant, if not the majority, of the entrepreneurship that

drive growth in the Cyber security market space. Many of them are entrepreneurial and come from innovation-oriented academic institutions such as MIT and Stanford where thousands of small businesses have been launched by current graduate students or recent graduates. Many of these small businesses have become centers of innovative and entrepreneurial ventures where technological groundbreaking is a regular feature.

The growth of many medium and big-sized firms is made possible by the entrepreneurship of small businesses. Thousands of these companies have peaked in their organic growth but continues to grow from mergers and acquisitions of highly entrepreneurial small businesses. Therefore, there is no doubt that the entrepreneurship of small businesses is the fuel that propels growth, consolidation and expansion of services in organizations that have peaked in their organic growth. In the last ten (10) years, it is worthy to note that countless numbers of small businesses that are in the Cyber security business have been acquired by large firms.

The role played by small businesses in strengthening Cyber security efforts in the United States can be measured by several metrics and indicators. But by most accounts, the impact of small business contributions to the Cyber security sector and the overall economy can be described in the broad terms of "Talent," "Capacity Creation," "Incubation," "Innovation," "Niche Services" to mention but a few.

1. **Talent** – Cyber Security is a field that has become highly specialized. Like the medical profession where there are general practitioners and specialists, in the Cyber security practice, we have those that specialize in Policy work, Certification & Accreditation, Security Engineering and Architecture, Analysts, etc. Small businesses with lower overhead structures are sometimes more capable of attracting and retaining niche talent.

2. **Capacity Creation** – Many Cyber security initiatives at the federal and state levels spur capacity creation of different business lines and activities. A case in point is the recent DFAR changes proposed by the DoD that will affect the entire DoD supply chain which consist of mostly small businesses. Creating services that these small companies can use will become extremely important (and lucrative for the companies that do it).

3. **Incubation** ( of Technologies, Business Processes and Practices) -

   Many Cyber security technologies, business processes, toolsets to mention but a few were incubated by one or a group of individuals working as small business entities that are engaged in Cyber security practice or elsewhere. Such incubations eventually grow into products, solutions and niche services that are eventually launched into the market place by the big companies that acquired them.

   In multiple instances, in one form or another, the concepts and ideas behind many Cyber security defense arsenals like the firewalls, intrusion detection

systems, virtual private network devices, etc. originated from small businesses or individuals who are practicing as independent consultants.

**4. Innovation**

Small businesses are often executors of complex projects. As prime contractors, subcontractors, independent consultants and employees they are central to ideas generation. Through the many complex projects they work on they often discover areas of process, product, toolsets, business process and technology that need improvement. For example, as lead users of business toolsets, small businesses often recognize deficiencies and go on to improving or innovating the toolsets. They can be viewed as a poster child for the concept of "user innovation" as defined by MIT's Eric von Hippel or "crowdsourcing" as coined by Jeff Howe in a June 2006 Wired magazine article about istockphoto (http://www.wired.com/wired/archive/14.06/crowds.html). In contrast to the traditional R&D model that characterize big firms' innovation machines, where billions of dollars are spent before anything meaningful comes out of the efforts, working on the frontline, small businesses are better at collecting customer inputs to innovate, a move away from the traditional R&D to where users drive innovation.

Small business driven Innovation come in different shades. "There are a lot of different things that fall under the rubric of innovation," says Vijay Govindarajan, a professor at Dartmouth College's Tuck School of Business and author of *Ten Rules for Strategic Innovators: From Idea to Execution*. "Innovation does not have to have anything to do with technology." In the 1990s, innovation by small businesses in the Cyber security market space centered mostly on developing the technologies, quality control and cost of addressing Cyberspace threats. Today, in consonance with the nature of Cyber security which has become a constantly shifting target, small business driven innovations now revolve around efficiency and rewiring them for creativity and growth. For example, Sourcefire, Inc. that developed one of the model intrusion detection systems was until a few years ago a small Cyber security firm. It created the "Snort" that was a basic model for intrusion detection systems. Today, it is a publicly traded company with many leading-edge Cyber security products. In the nineties when Snort was created, technology development was the main focus in the Cyber security market. Today, innovation has moved beyond defining the technology onto some other forms of perfecting existing technologies and products, improving techno-economic efficiencies and cost of operations among others. This is generally reflective of the trend across the industry and the contributions by small businesses in different innovative endeavors are by no means small in comparison to those that originate for big-sized Cyber security organizations.

Inherently, across the field, there are small businesses evoking all types of innovation. There are technology innovators, business model innovators, process innovators amongst other.

**5. Niche services**

Niche services are those services that require specialized expertise, setup and organization to deliver. The expertise is largely acquired outside the bounds of any formal or organized training organization. The most recognized niche service in Cyber security is ethical hacking services. Although many training institutions deliver some form of Cyber security training with ethical hacking content, it is known that ethical hacking expertise is largely acquired through other means that are outside the confines of a trainer classroom. The most famous hacker Kevin Mitnick did not acquire his hacking skills in the classroom but rather through his extraordinary talent. Today, individuals with such talents have organized their practice around small business consultancies that provide their highly specialized services to hundreds of big businesses, the defense and Intelligence establishments and others that are in constant need of testing their information systems for proof of resistance to hackers.

Today's burgeoning niche services have become business requirements arising from different needs. In some cases, the need arise unexpectedly where such services have not yet being incubated, matured or fused into organizational business units and outside the reach of the entity requiring immediately service. Organizing for service delivery then becomes a long term project and the immediate recourse is to small businesses that have the established capabilities to organize and deliver them. In Cyber security field practice, we have seen countless such situations where the big companies working as prime contractors are not able to provide certain niche services but rely on small business subcontractors or independent consultants to provide them. Inherently, niche expertise is a mainstay in small business day-to-day existence.

Given the above, it could be argued that the key elements in Cyber security development strategy is to focus on the strengths and core competencies of small businesses that will enhance the overall security posture of our nation. There will be much value in examining ways to strengthen Cyber security efforts in the United States especially examination of the dynamics that drives innovation and spurs growth in small businesses with good track records and viable potentials. These could very well be the spark that unleashes the innovative fire in small businesses engaged in Cyber security practice.

Despite the very strong and positive contributions of small businesses in strengthening Cyber security efforts in the US, there are still obstacles in realizing the full potentials of small business entrepreneurship. Like individual entrepreneurs and big businesses, they require government support.

With a supportive environment and a fully committed program, both legislative and otherwise, small businesses can continue to grow, expand and drive Cyber security efforts towards new heights. The government, in its efforts to support small businesses in Cyber security, should address obstacles that prevent them from increasing their contribution to the overall economic growth of the USA.

6

Such programs should provide high quality initiatives that are supported by a legislative mandate and should stipulate a certain percentage of small business share of all federal contracts awarded for Cyber security. Low interest loans to support innovation or niche projects will strengthen the managerial skills of prospective and current small businesses and assist them in selling their products and services to the government. The program should also facilitate access to information, counseling and new Cyber research initiatives.

Before I close, I want to thank Senator Cardin again for asking me to testify. I gained my U.S. citizenship in May, 2006, and I am honored to be recognized for my company's success, and to represent American Small Business entrepreneurs everywhere. I will be happy to answer any questions the Committee might have.

**CHARLES M. IHEAGWARA**

11610 Middleham Drive
Upper Marlboro, Maryland 20774

Phone: (301) 741-0664
E-mail: charlesi@sloan.mit.edu

**TECHNOLOGY MANAGEMENT EXECUTIVE:**

Product and Service Incubation, Branding and Launching; Business and Technology Strategy; Business Development; Marketing and Contracting; Executive Client Management; Cyber Security.

A recognized multifaceted, multi-lingual result-oriented technology management executive with 11 years of accomplishment-laden experience in the information technology industry driving achievement of the highest priority in sales growth, product/ service brand launch, market share, and Cyber security strategy and execution. Record of success in expanding and contracting. A key strategic and tactical driver in efforts that drove more than 10-fold growth for the Unatek brand, to over $7 million in net worth, Charles brings valuable marketing and business development knowledge and insight regarding the leadership and management challenges faced by small start up and growing companies and brand. Charles received top-rated management education from MIT and Harvard.

Prior to assuming the position of Chief Marketing and Business Development Officer at Unatek, Inc. a US government Information Technology contractor, he was the Chief Technology Officer responsible for the company's enterprise technology roadmap and development programs as well as consulting engagements for corporate clients. He led business development efforts with several notable successes including positioning Unatek as a major US government prime contractor and expanding corporate business lines, contracting and marketing services and the workforce. He also led client development and management efforts that resulted into the formation of several strategic alliances with leading technology companies.

Previous employments include stints at the Office of the Chief Technology Officer, DC Government, Lockheed Martin, KPMG, Aligned Development Strategies, Inc. (ADSI) and Edgar online, Inc working on NASDAQ projects.

As a consultant at OCTO, he was responsible for the management of the District of Columbia Computer Emergency Response Team. At Lockheed Martin, he was the lead consultant for the Enterprise Information Systems "Next Generation Intrusion Detection Systems" re-engineering project, as director of IT security services at ADSI, he managed the INFOSEC program of the District of Columbia HIPAA privacy project for the TCBA –ADSI – Bearing Point contractor group, and as a systems security administrator at Edgar online worked on corporate and NASDAQ Online Web services /Internet portal IT security programs.

He was an adjunct professor at Universities in the Washington, DC metro area between 2002 and 2007 and has published more than forty (40) papers in refereed international technical and scientific journals and conference proceedings. A Licensed Professional Engineer and an internationally known technology researcher whose work is widely quoted, Charles is a sought after speaker at several industry conferences.

Charles studied Management and Engineering from the Sloan School of Management and School Engineering and received a Master of Science degree from the Massachusetts Institute of Technology (MIT). He also attended Harvard Business School where he completed several business and entrepreneurial studies in satisfaction of the MIT degree requirements. He holds a Ph.D. degree in computer science from the University of Glamorgan, Wales, UK, a Master of Science degree in Minerals Engineering from the University of Minnesota, Minneapolis, Minnesota, USA, a Certificate in Environmental Management from George Washington University, and Bachelor/Master of Science degrees in Metallurgical Engineering from the National University of Science and Technology, Moscow, Russia. He also attended the Moscow Automobile and Civil Institute, Moscow, Russia, where he completed Preliminary Engineering and Russian Language studies.

He is the recipient of the 2007 Maryland-India Business Roundtable's "Business Innovator of the Year" award and a finalist of the "2011 Maryland State Business Incubator of the Year" award. He is also a member of the Microsoft IT Advisory Council.

Senator CARDIN. Well, thank you very much. Ms. Djamshidi.

**STATEMENT OF SARAH DJAMSHIDI, EXECUTIVE DIRECTOR, CHESAPEAKE INNOVATION CENTER**

Ms. DJAMSHIDI. Senator Cardin, thank you so much for holding this very important hearing on the role of small business in the cybersecurity area and——

[Discussion regarding microphone.]

Ms. DJAMSHIDI. So thank you for holding this very important hearing on the role of small business and in the area of cybersecurity. I am delighted to be here and provide a voice to thousands of small businesses that are working and innovating in this particular area.

By way of background, CIC is a unique business accelerator and incubator that is focused on the role of small business in the area of——

[Discussion regarding microphone.]

Ms. DJAMSHIDI. Okay, much better.

Senator CARDIN. Much better. Let us start all over again. Well, not all over again.

Ms. DJAMSHIDI. So let me begin by providing background information on CIC. Many speaker members here referenced Chesapeake Innovation Center, and so I am delighted to provide a little bit more background, and also offer a perspective from the small business side of the equation.

So by way of background, CIC is a unique business accelerator that is specifically focused on serving as a direct connection between users of technology, and that would be government agencies and system integrators, as well as the creator of those technology and innovation areas, so small businesses are leading the way in innovation in the areas of homeland, national, and cybersecurity areas.

CIC was formed in 2003 and is located in Anne Arundel County and has served as the nation's first business accelerator focused on homeland and national and cybersecurity areas. Since then, we have worked with more than 50 technology companies. These are all small businesses. We have incubated and accelerate them through various programs that we have.

And then the other program that I have provided more information in my written testimony on, which is basically a program called Tech Bridge, we have worked with more than 170 technology companies from across the country, as well as globally, and we have brought them here to the State of Maryland and we have showcased their innovative technologies in the area of homeland defense and cybersecurity in front of some of the system integrators and Government agencies, particularly major security stakeholders around the Fort Meade area. So I would be more than happy to provide more information on that.

CIC is a Anne Arundel Economic Development Corporation and we have shared great success since 2003. Our companies have raised more than $100 million in private capital. Our companies have also won more than $300 million in Government contracts. A number of them have been acquired along the way, and more importantly, one of them in particular, in the area of biodefense and

homeland security has gone public, and that is PharmAthene. So we are very proud of them.

So today we spent a lot of time talking about the fact that we live in a digitized society. We enjoy many good things like Facebook and iPad, but we also talked about the importance of cybersecurity in this new era, in protecting our data, and how it is more important than anything else, and also it has serious impacts in our socioeconomic and national security areas.

One of the keys things I wanted to highlight is that more than 90 percent of Government critical infrastructure is built and supported by the private sector. Mission critical systems are built by defense contractors, and increasingly, Government agencies are relying on the private sector-built networks and systems and solutions.

So the question is, where does small business come into that? With small business, the majority of the private sector, which is comprised of, as we talked about earlier, by small businesses, are developing these innovative cyber technologies and tools to be able to support and basically secure this critical infrastructure.

So we think that in this new era, innovative small businesses play a very key and important role in this whole dynamic, and organizations, public/private partnership organizations like CIC, that is a partnership between the county, the State, and Federal agencies, is a key component in that whole mix.

At CIC, we spent a lot of time understanding the market and looking at some of the issues that small businesses face, some of the things that are important to you and we have talked about already here today. We understand there are a number of gaps in the marketplace, and so we have created a number of programs specifically designed to help small businesses navigate through those issues. And again, I have provided more detailed information in my written testimony.

Some of the programs to highlight include, for example, number one, we provide hands-on support and access to funding and Government opportunities. We have created a three-year long rigorous company building process where we navigate some of these small businesses. Again, the ones that are working on, as Senator Mikulski remarked, the geek companies, the technology companies that are developing unique innovative technologies in the areas of homeland and national and cybersecurity and helping them cross the chasm, if you will.

It is a difficult task to do and we serve through our partnerships. We bring in a lot of resources to be able to do that, and we partner with a lot of organizations across the State of Maryland in order to provide that.

Second, again, in partnership with various academic institutions that includes the community colleges, it includes the major academic institutions around the State, and various other organizations like Workforce Development Corporation, we bring in some of this training and education so that we can create those next generation cyber warriors and fuel the innovation inside some of these technology companies.

And then third, we have created various programs to bring the public and private together and showcase some of these innovative

technologies. Today some can argue there are no effective, or there are not that many effective, ways of bringing some of these innovations to the marketplace. So they can actually see the light of the day and go solve tough problems.

We have created specific programs to do that, and that is the program that I referenced earlier as Tech Bridge, and through that, we look across the country. We have screened and vetted hundreds and hundreds of companies. And then we bring in more than—we have brought in more than 180 companies to date to the State of Maryland, showcased their innovative technologies to major stakeholders such as the National Security Agency and other agencies, and we have brought those innovations here to the State of Maryland.

We think that is a great attraction tool. We hope that some of these companies will think of the State of Maryland as either their expansion area or their home, for example.

Finally, in support of the entrepreneurship culture around the region, we think that is an important thing to do and we play a key component in that. And so, we have launched several programs, one of which, for example, is the Business-to-Government CEO Roundtable which is meant to put our finger on the pulse of small business issues and understand that and create value-added services in partnership and help with others and bring those to the small businesses.

One of the key things I wanted to highlight is that I talked about our companies historically have raised or brought hundreds of millions of dollars in private capital and Government contracts. But I want to share with you one very recent example.

One of our current companies in our portfolio, Inovex Information Systems, is a small company headed by three first-time entrepreneurs who serve Fort Meade, works in the area of cybersecurity and support in that region, and this company came to us in 2009 with 13 employees. Today they have not only quadrupled their revenues, but they also employ more than 43 highly-skilled workers.

So that is a great example that is very close to home. It is probably one of the best kept secrets, and I definitely wanted to share that with you. Is that all, enough, to your point? We think there is more work that can be done. And are we doing it all? I do not think so. And so, with that, I think a lot of people touched on it, and you also mentioned it.

We think that access to capital is absolutely huge and crucial toward continuing the innovation and bringing these technologies to the marketplace. We also think support for public/private partnership organizations also is important in support of the small businesses because this is a huge task that is going on.

And finally, I think in observation of what is going on, I think it is crucially important for various counties, agencies, Federal, State, what have you, to work in close collaboration with each other so that we can continue this innovation in the area of cybersecurity that is so important to us. And then I will take any questions.

[The prepared statement of Ms. Djamshidi follows:]

CHESAPEAKE Innovation Center

Written Testimony of Sarah Djamshidi to the United States Senate

**"The Role of Small Business in Strengthening Cybersecurity Efforts in the United States."**

## Senate Committee on Small Business and Entrepreneurship

**Laurel, MD Field Hearing**
**Senator Benjamin L. Cardin, Maryland**

July 25, 2011

On behalf of
Chesapeake Innovation Center
www.cic-tech.org

Sarah Djamshidi
Executive Director
**Chesapeake Innovation Center**
175 Admiral Cochrane Drive
Annapolis, MD 21401
Tel 410.224.2030
Cell 410.212.4150
Fax 410.224.4201
sdjamshidi@cic-tech.org
www.cic-tech.org

*Introduction*

My name is Sarah Djamshidi. I am the Executive Director of the Chesapeake Innovation Center ("CIC"). Senator Cardin, thank you for holding this very important hearing on the role of small business in cybersecurity and for offering us the opportunity to discuss the small business issues. I am honored to submit written and verbal testimony to you and this esteemed subcommittee.

CIC is a unique business incubator and accelerator designed to serve as the direct connection between major users of technology and the early-stage technology companies that are leading the way in innovation. Whether we're scouting for breakthroughs or vetting and supporting the companies behind them, we make it our business to stay in the know. That's why we are able to bring the expert guidance, tangible value and increased efficiencies that accelerate progress on both sides of the innovation equation.

CIC, formed in 2003 and located in Anne Arundel County, has served as the nation's first business accelerator for homeland, national and cyber security areas. CIC has focused on the intelligence community. In addition, CIC has played a key role in fostering innovation in support of homeland and cybersecurity efforts with strong ties to the national security stakeholders, working with more than 50 emerging technology businesses in the State of Maryland and more than 170 emerging technology businesses from around the country and the globe. CIC is a program of the Anne Arundel Economic Development Corporation ("AAEDC"). AAEDC is the designated organization for supporting economic development and growth for the Anne Arundel County.

CIC has enjoyed significant success since 2003. As examples of our success, CIC member companies have raised more than $100 million in private capital and more than $300 million in government contracts. In addition, PharmAthene (AMEX:PIP), one of CIC's graduate companies went public.

**Background and Rationale for CIC's Unique Programs**

Today we live in a highly digitized world. Social networking and instant messaging accounts are exploding. By the end of 2010, The Radicati Group projects that there will be 2.2 billion social network accounts worldwide, and currently, 2.4 billion instant messaging accounts. By 2014, they project that there will be over 3.7 billion social networking accounts and over 3.5 billion instant messaging accounts. In 1996, there were 16 million Internet users worldwide. Today, there are more than 1.8 billion Internet users across the globe. In 2009, there were a total of 90 trillion e-mails sent. And in 2010, around 247 billion e-mails sent every day. Of those 247 billion e-mails, 200 billion were spam. The digitized world has brought on a lot of good things (Kindel, ipad, facebook, etc..), but it also poses tremendous vulnerabilities, our data must be protected.

On Thursday, July 14, 2011, the Pentagon revealed that in the spring it suffered one of its largest losses ever of sensitive data in a cyber attack by a foreign government. William Lynn, the deputy secretary of defense, indicated that 24,000 files containing Pentagon data were stolen from a defense industry computer network in a single intrusion in March. This combined with cyber attacks on Estonia and cyber attacks during the 2008 Georgian incursion have served to increase awareness that cybersecurity is not just about protecting computers, but also has implications for U.S. national security and economic well-being. As a result, cybersecurity has climbed to the top of the list, making it one of the key concerns facing our digital society. As we all agree, in today's digital age, individuals, and nations are increasingly capable of applying "cyber warfare" techniques against both public and private computer-based systems (from military systems to private power grids, banks, hospitals, air-traffic control systems, etc...). Currently, the DoD computers alone receive about 6 million attempted penetrations every day! These attacks are extremely difficult to trace back to their sources; and, at the same time, are becoming increasingly sophisticated in their tools and techniques. In addition, it is important to note that more than 90 percent of government critical infrastructure is built and supported by the private sector and more than 80 percent of the logistics are transported by private companies. Mission-critical systems are designed, built and often maintained by defense contractors. Thus, the government relies on private-sector networks and capabilities. Where do small businesses come in? Within the private sector the majority of the cyber technologies to protect our nation and critical infrastructure are built by small businesses.

Today, most cyber work is manual and preformed by individuals. Since there is a significant shortage of qualified cyber experts, the task of protecting our nation becomes a daunting task. In addition, *the one consistent theme is that the cyber defenses commonly used today are simply not effective against most forms of advanced cyber attacks*. Increasingly, the government agencies require advice, assistance, coordination and products to support the operational planning and execution and technology development required to assure superiority for the war fighter in the cyber domain.

Innovative small businesses can hold the key to success in this new era and public-private partnership organizations such as CIC (in partnership with county, state and federal agencies) can in-turn support them. It is important to note here that currently, there are no effective processes or mechanism by which small businesses can present their innovative cyber technologies to the market. CIC, along with its partners in the region is attempting to build such bridge.

As we know, technical innovations are a key catalyst for economic growth, and advancement in national security, public safety and healthcare. In most parts of the Washington, DC region, including Maryland, a significant gap exists between entrepreneurs creating viable early stage companies and a viable small business capable of brining technology-based products to the market place. This gap exists for a number of reasons:

(1) Professional and educated workforce;

(2) An inadequate amount of seed and early stage funding for technology and product development, as well as for start up and working capital;
(3) Many technology entrepreneurs are not sufficiently educated in business related topics.

AAEDC and CIC have closely examined many of these obstacles, and have developed a comprehensive plan to accelerate the growth of the technology companies, via unique programs, here in Anne Arundel County and in the surrounding region.

This plan encompasses four components: (1) hands-on support and access to funding and government opportunities; (2)Education and support for a more robust workforce (3) strategic relationships between private and public sector in support of innovation in the area of cybersecurity; (4)entrepreneurship culture building.

**CIC's Hands-on Support Approach and Benefits**

Hands-on assistance and support in addition to access to government and funding opportunities are paramount in building a successful ecosystem where new innovative cyber tools and methods are born, supported and eventually deployed. The CIC program selectively admits 2-4 new startups per year pursuant to a thorough criteria. During a typical three-year acceleration and incubation period, CIC applies a rigorous company-building process to help advance the growth of the emerging technologies companies into viable, well managed, properly funded ventures. CIC mentors and marshals resources in partnership with AAEDC, Anne Arundel County, the educational institutions, venture capitalists and other resources from around the region to assist its member companies with (1)business planning and market analysis, (2)capital formation, (3)access to government opportunities and business development, (4) marketing and PR. CIC helps keep its portfolio companies on track to commercialization through weekly status meetings and consistent hands-on participation.

A summary of the benefits of working with the CIC include:

- **CIC Resource Network** – small businesses can expand their business-building network through CIC's contacts within the region, including leading corporations and institutions, technical expertise, staffing pools, professional services and other valuable sources of business assistance. Within the Washington, D.C. and mid-Atlantic region are numerous defense contractors and integrators who may have an interest to work with the CIC member companies and CIC will make introductions as appropriate.

- **Peer-to-Peer Program** – small businesses who are members of CIC can benefit from participating in the CIC's diverse and collaborative community of early stage companies all focused on the National Security marketplace. Share resources and contacts with other like-minded entrepreneurs and leverage the CIC's unique synergy dynamic.

- **Coaching and Mentoring –** CIC member companies receive one-on-one assistance from experienced entrepreneurs and technical experts within the CIC Community. The CIC

Management Team becomes part of the small business founding team and marshals its extensive resource network to help drive fulfillment of mutually established business objectives.

Entrepreneurial ventures depend on new inventions. One way to track the propensity to invent is through patent filings. A study released by the U.S. Small Business Administration's Office of Advocacy shows that 40 percent of the companies that issued at least 15 patents over a five-year period were small businesses. This and other studies show that small businesses are more likely to develop emerging technologies than their larger counterparts. **Thus, small firms are actively engaged in the cutting-edge technologies that will shape the nation's future growth.** Early stage commercial technologies are more than willing to implement Intelligence community-specific features because it opens a new market for them. However, they quite often do not have the market understanding to do so. Through our expertise and historical work at the Chesapeake Innovation Center (CIC), we have found that fine-tuning capabilities in emerging commercial technologies reduces risk, cost and time-to-market by orders of magnitude compared to conventional technology development methods. We believe that it's easier to leverage a technology to meet agency requirements than build it from scratch. Cyber Stakeholders will benefit from our finger-on-the-pulse approach to identifying relevant emerging technologies, as well as from our in-depth knowledge of intel and cyber community requirements.

- **Investor Prep and Network – Small Businesses** who are members of CIC receive iterative feedback by the CIC Management Team on how to effectively prepare for and present to investors, and gain introductions to our quickly expanding network of equity investors inclined to invest in ventures around innovative technologies.

- **Direct Partner Channels & Business Development**– Through its growing list of Partners, the CIC is able to create direct access for its members to decision makers within select leading organizations in the National Security Sector. Our customer network includes NSA, DHS through preferential mentor-protégé relationship, Boeing, Northrop Grumman, and ARINC. In addition, we have dedicated business development resources to assist CIC member companies in reaching government customers.

- **Marketing and PR Leverage** – The CIC has established itself as the nation's premier technology accelerator for National/Homeland and Cyber Security. CIC has established relationships with various regional and national members of media and press. As appropriate for each venture, these relationships can be leveraged to provide exposure for the CIC portfolio companies.

**Education and Support for a More Robust Workforce**
**Augmentation of Cyber Workforce & Job Creation – Developing Tomorrow's Cyber Warriors**

CIC has leveraged its close link to the Cyber Stakeholders at Fort George G. Meade and works closely with AAEDC, Anne Arundel Community College ("AACC"), Anne Arundel Workforce Development Corporation ("AAWDC") to educate the next generation of cyber workforce and other educational institutions in the State of Maryland. Innovation and entrepreneurship will be crucial to the nation's economic revival and competitiveness in a global marketplace. A 2008 update by Zoltan Acs, to David Birch's seminal research of the 1980s and 1990s on **"gazelles" which are fast-growing, high-impact firms (classically defined as a company growing at an annual rate of 20% or more), found that these firms account for almost all of the growth in private sector employment and revenue in the economy.** With respect to job creation, since the mid-1990s, small businesses have generally created 60 to 80 percent of the net new employment. **As one-third of US workers are employed by the small business sector, CIC will focus on the cyber training needs for small businesses, empowering them to maintain and to hire a more educated workforce.** To that end, in partnership with AAEDC, CIC can assist small businesses with workforce training. Through the AAEDC Workforce Training Partnership, eligible companies can gain the critical skills upgrades or technical training for employees that will improve overall productivity and competitiveness. An established and successful relationship with Anne Arundel Community College and the Center for Workforce Solutions as well as other training providers, helps AAEDC accomplish this training. Training can occur at the workplace, or the Anne Arundel Community College campus in Arnold, or at specialized labs at Arundel Mills and the Glen Burnie Town Center. In addition, CIC actively introduces its members and other small businesses to the Pathways to Cyber security Careers which was funded by a $4.9 million Community-Based Job Training grant to Anne Arundel Workforce Development Corporation, Anne Arundel Community College and their partners over a period of three years for the Pathways to Cybersecurity Careers Consortium initiative. This project will address the challenges of a lack of adequate pool of skilled cyber workers, the shortage of laboratory facilities to support cyber training, a lack of training in flexible modalities, and barriers to learning for under-served populations.

**Strategic relationships between private and public sector in support of innovation in the area of cybersecurity**

**Attraction of "best-of-Breed" Technology Companies to the Sate of MD**

CIC's leadership, know-how, unique set of business assistance offerings and connection has provided a great attraction tool in bringing best-of breed technology companies to the State of Maryland. This will in-turn lead to the attraction of some of these emerging technology companies to close proximity of Cyber Stakeholders and growth/job creation for the State of Maryland. CIC's proprietary and established attraction screening program, ***TechBridge***, has

screened, vetted and attracted viable emerging technology businesses to the State of Maryland. Through TechBridge, hundreds of companies have been screened throughout the nation and more than 170 companies have come to Anne Arundel County, MD, to present their capabilities to the defense system integrators and federal agencies such as NSA. To date, 48% of companies participating in the TechBridge program have been from across the country.

**Entrepreneurship Culture Building**

CIC has developed a number of programs to foster entrepreneurship culture in the region. One of these programs is the Business-to-Government (B2G) CEO Roundtable. This program is designed to bring CEOs, and company founders of emerging technology companies currently serving the federal government (or those who would like to expand their business to the public sector) together for a dynamic exchange of information and dialogue on the issues that are currently facing small businesses. This group gathers in a board-room setting and engages in a dynamic conversation with great speakers (former government executives, great entrepreneurs, and business experts with deep experience in building hyper growth companies), all focused on tackling real issues facing most small businesses in the market.

**Results & Examples**

The CIC programs has enjoyed significant success since 2003: (1) over 40 companies have been successfully accelerated and incubated; (2) over $300 million in government contracts have been secured by CIC firms; (3) over $100 million in private capital has flowed into CIC companies; (4) CIC has brought more than 170 high tech small firms to the region and has showcased their technologies to the government agencies and system integrators; and (5) CIC firms have been acquired and one company, PharmAthene, serving the homeland security market, has gone public. PharmAthene, a biodefense company, together with its subsidiaries, engages in the development and commercialization of medical countermeasures against biological and chemical weapons.

In addition, current CIC firms continue to thrive as well. For example, Inovex Information Systems, a promising Veteran Owned Small Business (VOSB) company serving Fort Meade customers, became a member of the CIC in 2009 with 13 employees. Today, they have almost quadrupled their revenues and currently employ more than 43 highly skilled workers. Among other cutting-edge services, they provide cyber support to their customers at Fort Meade.

**Recommendations**

1. Increase the amount and types of funding available to small businesses to continue innovation, create jobs and secure our nation;
2. Increase the amount of support that is available to small businesses. Support public-private partnerships as one of the successful mechanisms.
3. Better collaboration between Federal, State, Counties, academic institutions, funding agencies, venture capitalists, the private sector, and different members of the entrepreneurial community to better foster innovation in this key area, Cyber security. Today, it seems that our efforts are fragmented.

CHESAPEAKE Innovation Center
America's first business accelerator for homeland and national security

**Sarah Djamshidi**

**Executive Director, Chesapeake Innovation Center (CIC)**
**President, Maryland Business Incubation Association (MBIA)**

As the Executive Director, Sarah Djamshidi oversees all the Chesapeake Innovation Center (CIC) activities, coaches and mentors the member companies. CIC is a unique venture accelerator that connects promising technology companies and emerging technologies with government agencies, major government contractors and private sector customers. CIC focuses on homeland, national and cyber security markets.

Prior to her appointment at the CIC, Ms. Djamshidi served as Director of the University of Maryland Technology Advancement Program (TAP), the first technology venture incubator in the State of Maryland. TAP partners with regional entrepreneurs and provides extensive hands-on support to build early-stage technology companies. During her tenure, $20 million was raised for portfolio companies. In this role, Djamshidi actively advised TAP portfolio companies on market research, business and strategic planning, business process reengineering, financial analysis, business development, recruiting and fundraising. In addition, Djamshidi oversaw all operations of TAP and managed company selection and lead the due diligence activities. Moreover, she helped in the design, development and implementation of the University of Maryland's first technology spin-out program, MTECH VentureAccelerator.

Ms. Djamshidi has been an adjunct professor and lecturer with *A. James Clark School of Engineering* and University of Maryland's Honors Program, teaching undergraduate classes in technology entrepreneurship. In addition, she is a frequent speaker on venture incubation practices at national conferences. Ms. Djamshidi is a board member for the William James Foundation, where she helps the foundation in forming strategies and serves as a judge for the foundation's national Socially Responsible Business Plan Competition. She is also an economic and business evaluator for the National Science Foundation where she helps in the selection of Phase I and Phase II SBIR awardees. In addition, Ms. Djamshidi currently serves as the President of Maryland Business Incubation Association (MBIA) which is a network of more than 20 incubators and accelerators supporting more than 400 emerging companies throughout the State of Maryland.

Previously, Ms. Djamshidi launched a graphic design and communications unit of the University of Maryland. In this capacity, she directed client projects, set pricing, and conceptualized creative campaigns for various organizations. Additionally, she has grown and launched businesses and managed a variety technology organizations.

Djamshidi has a degree in Management Science and Statistics with specialization in Decision Information Systems from the University of Maryland.

Senator CARDIN. Well, thank you very much for that testimony. Dr. von Lehmen.

**STATEMENT OF GREGORY VON LEHMEN, Ph.D., PROVOST, UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE**

Dr. VON LEHMEN. Thank you, Senator Cardin. On behalf of the University of Maryland University College, I thank you for the opportunity to appear in this field hearing of the Senate Committee on Small Business and Entrepreneurship. Both you and Senator Mikulski have alluded to the threat in this area of cybersecurity.

I have been invited here to talk about how the University of Maryland University College is working to meet the workforce need in this area, particularly in educating cybersecurity professionals, many of whom we believe will use their knowledge to further small business expansion, both here in Maryland and throughout the United States.

In my capacity as Provost, I led a very talented academic team, starting about 18 months ago, to launch three cybersecurity degree programs in collaboration with an advisory board of public and private sector industry leaders, many of whom had a long background and distinguished career in the Department of Defense and the military services.

Thanks to their tremendous input, our programs are specifically mapped to professional expectations in industry and government, which is an important distinction when it comes to effectively meeting critical State and national workforce needs.

As the largest public university in the United States, by head count, and one of the 11 degree-granting institutions within the University system of Maryland, UMUC was created 64 years ago to meet the unique academic needs of working adults, most of whom return to college for professional advancement.

Today we serve 94,000 students in all 50 States, 28 countries, including some 40,000 active duty members, veterans, and their families. We do this face-to-face at more than 150 locations around the world, and also, online through our award-winning virtual campus.

We are supportive of opportunities for both emerging and established small business owners through our association with the Minority Business Enterprise, whose award ceremony UMUC hosts each and every year, and our NBE-endowed scholarship fund which was established last year with awards to be made this coming academic year.

In responding to the urgent needs for tens of thousands of cybersecurity professionals nationwide, the University of Maryland University College stepped forward to meet the challenge, becoming a key player in Governor Martin O'Malley's plan to position Maryland as the country's epicenter for cybersecurity, and to be sure our university is exceptionally well-positioned to shape the course of cyber education going forward, given its healthy track record and IT program development, its ongoing relationships with the Department of Defense, Federal agencies, and contractors, and its large contingent of clearance-ready students.

What is more, UMC is one of 147 colleges and universities in the United States to be designated as an NSA DHS Center of Academic Excellence in Information Assurance Education, and more recently,

we have begun working with the National Institute of Standards and Technology on its NICE initiative which is to create a taxonomy of cyber work roles and then to map curricula to those work roles. We think this is a very important effort to create a common reference point for academic programs in cybersecurity.

Consequently, in developing its cyber initiative, the university created two master degree programs, one in cybersecurity and one in cybersecurity policy. And additionally, the university offers a bachelor's programs in cybersecurity and a number of graduate and undergraduate certificates. All three degrees and these certificates offer a market-driven curriculum and are furnished primarily online.

We have also recruited an exceptional group of faculty members. We have built a remote access cyber virtual lab which can accommodate up to 800 concurrent users. We have raised $1.2 million for cybersecurity scholarships, and we have signed articulation agreements with community colleges in Maryland and Louisiana that offer associate degree programs in cybersecurity to help create this pipeline of educated professionals.

In less than a year—in less than a year, we have enrolled close to 2,200 cybersecurity students, nearly half of whom are completing one of two graduate degree programs that I mentioned, or one of the certificates in this field.

The vast majority of our graduate students, about 89 percent according to a recent survey of our students that we conducted, around 89 percent have at least five years professional experience in IT Information Assurance or computer security in Government or across sectors of the economy, while 61 percent of them hold security clearances.

Moreover, a significant number of these enterprising students will undoubtedly use their new skills to launch businesses of their own. And I close with two examples. One of our graduate students in the technical track are MS in cybersecurity, wants to start his own cybersecurity consulting firm working with private corporations.

He is currently employed as an executive at a large firm, but he plans to start his own consulting practice. And having more than 27 years experience in military intelligence, he is now acquiring the additional technical skills through our program that he needs to launch his new business.

And another of our graduate students, which I just happened to meet by chance last week at an AFCEA conference, is in our master's of cybersecurity policy. He started his own communications firm in 2006, focusing on public relations, corporate and social responsibility planning, and digital content strategies.

His firm is not a cyber company yet, but as he says, and I will quote, a comment that he makes, his vision is to focus on the prevention, policy, and people side of cyber. Policy development, implementation, and communications, he notes, are so critical to the success of any organization, end quote.

These two students in their maturity and in their drive well represent our student population as a whole, and I believe will make a significant contribution to small business development in this State. So once again, Mr. Chairman, I appreciate this opportunity

to speak before the Committee and I am happy to answer any questions that you might have.

[The prepared testimony of Dr. von Lehmen follows:]

University of Maryland University College
*Office of the Provost*

**Written Testimony**
**US Senate Committee on**
**Small Business and Entrepreneurship**
**July 25, 2011**

Good morning Chairman Cardin and members of the Small Business and Entrepreneurship Committee. I am grateful for the opportunity to speak with you about the University of Maryland University College (UMUC) and its commitment to educate cybersecurity professionals with advanced skills, a significant number of whom will use their knowledge to further small business expansion, both here in Maryland and throughout the United States.

I am Dr. Greg von Lehmen, and as Provost of UMUC, I led the university's successful efforts to launch three cybersecurity degree programs, in collaboration with a team of public and private sector industry leaders. Thanks to their tremendous input, these programs are specifically mapped to professional standards and expectations in this high demand field, an important distinction when it comes to effectively meeting critical state and national workforce needs.

As the largest public university in the United States, and one of 11 degree-granting institutions within the University System of Maryland, UMUC was created 64 years ago to meet the unique academic needs of working adults. Today, it serves 94,000 students in 28 countries and all 50 states, about 40,000 of whom are active duty military service members, veterans, and their families. These remarkable men and women take classes onsite in more than 150 locations – including military bases in Iraq and Afghanistan – and online through our award-winning virtual campus, one of oldest, largest, and fastest growing in the world.

For the most part, UMUC students are in their thirties and forties. Four out of five of them work fulltime; nearly half are married with children; more than half are women; and well more than one-third are self-identified minority group members. Unlike their traditional, college-aged counterparts, the vast majority of them are seeking academic opportunities that support professional advancement in their chosen fields. And in tough job markets such as this one, many of these students want to change careers altogether.

Consequently, in providing them with highly marketable credentials, UMUC has developed an academic model that enables it to rapidly respond to critical

*3501 University Boulevard East, Adelphi, MD 20783-8001 USA*
*301-985-7174 • Fax 301-985-6432 • www.umuc.edu*

workforce development needs, *as* and *where* they emerge, with career-ready degree and certificate programs. With that in mind, the university uses two proven strategies to ensure that these programs are up to speed. In identifying appropriate learning outcomes and designing suitable curriculum, UMUC's academic leadership works closely with its vast network of public and private sector industry learning partners, which include many of the area's largest government agencies and corporations. Moreover, UMUC relies heavily on adjunct instructors, who as "scholar-practitioners," are experienced knowledge leaders in their fields. These distinguished faculty members boast academic credentials from some of the world's leading universities, and many of them have attained regional, national, or international recognition for their professional accomplishments. In addition, sixty-nine percent of our faculty members hold doctoral or other terminal degrees.

Over the years, UMUC has helped thousands of its students spread their entrepreneurial wings by investing in academic programs and resources, designed to furnish them with both the relevant knowledge and the practical skills they need to effectively run their own businesses. The university is especially proud of its Entrepreneur Development Center at Dorsey Station, a joint project with three of the Washington Metropolitan area's most successful independent businesspeople.

This center provides continuing education and professional networking opportunities for small business owners interested in broadening their entrepreneurial horizons. UMUC also administers a special Minority Business Enterprise scholarship fund, and co-sponsors Maryland's Top 100 Minority Business Enterprise Award, in conjunction with the Governor's Office of Minority Affairs and the Maryland Chamber of Commerce.

UMUC began offering leading-edge computer science and information technology degree programs as the demand for qualified IT professionals began to escalate, a trend that spawned an abundance of small businesses in Maryland. Moreover, given UMUC's proximity to and ongoing relationships with such federal agencies as the National Security Agency, the Department of Defense, and the Department of Homeland Security, the university has become a leader in information assurance education.

In fact, UMUC is one of only 147 institutions out of more than 4,300 U.S. colleges and universities to be designated as a National Security Agency/Department of Homeland Security Center of Academic Excellence in Information Assurance Education. As such, the university provides academic coursework that is designed to meet federal agency standards in this specialized discipline.

Not surprisingly then, cybersecurity was the natural next step in expanding UMUC's already solid portfolio of IT-related degree and certificate programs, especially given the projected need for highly skilled cybersecurity professionals to fill tens of thousands of jobs, many of which will be located in Maryland. This burgeoning field also offers tremendous growth potential for small business owners interested in providing contractual cybersecurity services to public agencies, private corporations, and non-profit organizations.

Upon scanning the higher education landscape, UMUC's academic leadership found that there were certainly other respected universities conducting research and/or furnishing coursework in information security. None of them, however, offered undergraduate or graduate degree programs specifically in cybersecurity, despite strong recommendations for such workforce development options from the CSIS Commission on Cyber Security for the 44th Presidency and the Maryland Department of Business and Economic Development.

Consequently, in meeting the challenge, UMUC worked closely with a group of nationally recognized, public and private sector industry leaders, to map its curriculum against professional standards and expectations in the field. This effort produced two master of science degree programs in Cybersecurity and Cybersecurity Policy, as well as a bachelor of science degree program in Cybersecurity, all of which are furnished predominantly online to maximize student outreach and enrollment capacity.

Designed to prepare *complete* professionals, armed with advanced skills in secure system design, strategic cyber defense, and public policy development, these programs offer both a market-driven curriculum and an interactive learning environment. UMUC has also built a remote access Cyber Virtual Lab, which affords students a unique opportunity to experiment *from a distance,* using real world scenarios and hands-on applications to detect and combat simulated cyber attacks. And like the university's acclaimed Systems Security Lab, it was developed by Dr. Jim Chen, UMUC's information assurance program director and a University System of Maryland Faculty Member of the Year Award winner.

Likewise, UMUC has recruited an exceptional group of scholar-practitioners for its cybersecurity faculty. This faculty comprises such recognized experts as Dr. Joon Sun, who came from the Johns Hopkins University Applied Physics Lab, where she worked as an information security research engineer, and Dr. Christopher Feudo, who is developing a secure enterprise architecture for the National Nuclear Security Administration. UMUC has also signed "two plus two" articulation agreements with several community colleges that now offer associate's degree programs in

cybersecurity, including Anne Arundel Community College and Howard Community College in Maryland, and Bossier Parish Community College in Louisiana.

UMUC plays a key role in supporting Governor Martin O'Malley's plan to position Maryland as the nation's epicenter for cybersecurity. In conjunction with the Anne Arundel Workforce Development Corporation, the university provides academic support to individuals interested in pursuing professional certifications in the cybersecurity field.

Additionally, it is an active member of the Pathways to Cybersecurity Careers Consortium, which includes a significant number of regional IT firms, several local community colleges, and such state agencies as the Maryland Department of Business and Economic Development and the Maryland Governor's Workforce Investment Board. UMUC also serves on the advisory board for the homeland security program at Meade High School (on post at Fort Meade), which is mapped directly to the cybersecurity program at Anne Arundel Community College.

Now less than a year after launching its cyber education initiative, UMUC has received widespread recognition for its efforts, including a prominent mention in the November 2010 report from the CSIS Commission on Cybersecurity for the 44th Presidency. It has built a dedicated cybersecurity scholarship fund in the amount of $1.2 million; and was selected by the Armed Forces Communications and Electronics Association, or AFCEA, to serve as its exclusive provider for online cybersecurity programs.

Even more impressive, since unveiling its new programs, UMUC has already received more than 3,500 applications, and enrolled close to 2,200 students, nearly half of whom are completing one of the two graduate degree programs in cybersecurity. According to a recent survey, around sixty percent of these graduate students have five years or more professional experience in IT, while twenty-nine percent report spending at least five years working in information assurance, computer security, or cybersecurity.

Well over half of these students, or fifty eight percent, are currently employed by the military, the Federal government, or one of its many independent contractors; and another twenty percent of them work in the non-governmental private sector. In addition, half of those surveyed had earned an industry or professional certification in their field, and sixty-one percent held a security clearance.

Of course, given past experience, UMUC knows that at least some segment of these enterprising men and women are interested in using what they learn to launch their own businesses.

For instance, one of our graduate students is pursuing his master of science degree in cybersecurity as a prelude to starting his own Maryland-based consulting firm down the road, after spending more than 27 years as a civilian employee with the U.S. Navy, where he worked in intelligence security. And while he has gained solid experience on the cybersecurity public policy side, he wants to acquire the technical skills he will need to provide private corporations with a full spectrum of cybersecurity consulting services. In the meantime, he continues to hone his business management expertise as an executive with one of the Washington area's large government contracting firms.

Yet another one of UMUC's graduate students plans to enter the small business arena, once he finishes his master's program in cybersecurity. A 20-year military veteran, he now works on the civilian side, as a federal contractor in the communications security area. After completing his degree, he hopes to explore his entrepreneurial side, as an independent business owner in Hagerstown, Maryland, building secure information systems.

And as always, UMUC will continue to support their professional goals in the years to come, by providing these outstanding students with other academic programs and resources they may need to operate their businesses successfully.

# Greg von Lehmen, PhD

## University of Maryland University College

Dr. Greg von Lehmen serves as provost and chief academic officer at UMUC. He joined UMUC as the area director for Japan in August 2001, and worked for UMUC Asia as area director for Japan for four years. He returned to the United States in 2005, where he has served as the senior associate dean within the School of Undergraduate Studies and later as senior vice provost.

Prior to joining UMUC, Dr. von Lehmen taught constitutional and administrative law, political philosophy and public administration for five years at Georgia Southwestern State University, where he was a tenured associate professor. He joined Troy University in 1990, serving initially as assistant professor of public administration in the university's Master of Public Administration program in Europe and teaching in Germany, Spain, England, Italy, Turkey, and Portugal. He returned to the United States to serve as regional director of University College Programs–Southwest, managing Troy's programs at military and NASA facilities in New Mexico, Arizona, and Montana. In 1997, he relocated to Okinawa, where until 2001 he oversaw Troy's graduate programs in Japan, Korea, Guam, and Hawaii.

Dr. von Lehmen holds a PhD in political science and an MPA from the University of Georgia. He earned his BS in economics from Northern Kentucky University.

Senator CARDIN. Well, once again, let me thank all three of you for your testimony and your contribution to this hearing.

Dr. von Lehmen, I found your presentation concerning the demographics of your student body as it relates to cybersecurity programs to be very interesting. You have the largest program in our country from the point of view of a public university and your student body.

Can you share some more information? That 61 percent seemed like a high number. Is that an increase? That is who had clearance, I think you used that.

Dr. VON LEHMEN. That is correct, sir.

Senator CARDIN. Has that been running? Have you done studies about that in previous years? Is that a number you think is increasing or decreasing?

Dr. VON LEHMEN. Our cybersecurity programs were launched the fall of last year, and so, this is the first survey of that student population. We do not have historical comparative data.

Senator CARDIN. Did that number surprise you or did you expect that it would be that high?

Dr. VON LEHMEN. I must say we were surprised that we had such a large number of individuals already cleared, but we attribute that to the mix of military students who are in our program, as well as those civilians who are working in the information assurance field for the Government or for contractors.

Senator CARDIN. And, of course, these are students that are enrolling in both undergraduate and post-graduate programs?

Dr. VON LEHMEN. Our baccalaureate program and our master's programs.

Senator CARDIN. Right. Can you tell us more about the demographics or can you supply them to the Committee, like age, employment background?

Dr. VON LEHMEN. I would be happy to provide that information about our cybersecurity students, in particular, but I am fairly confident in saying that the profile of that student body probably matches very closely with the general profile of our student body.

The average age is 32; they are more likely to be married than not, more likely to have children than not, more likely to already be employed than not. And so, these are students who want to advance their career in some way, either within their current employment or by changing their employment, and who have made a very serious decision to go back to school.

One of the things we tell corporations, and we meet with many of them in the cybersecurity sector, is that our students are very special. They made a decision to get into this field because they see a future in it, because they see the threat to our nation and they are committed to making a difference.

It is more likely that if they are employed by one of these firms, they are not going to be leaving, but will make a commitment to their work in that firm.

Senator CARDIN. I think it is very encouraging, and, of course, there is a great advantage to us here in Maryland, although I know your program is international, that your student body is global, basically.

Let me change gears a little bit to Dr. Iheagwara and to Ms. Djamshidi. You all put a face on this issue. You started talking about specific companies and, of course, your company which I think is very helpful because we hear more about the statistical information so it is good to see the specific companies that you talk about.

And you talked about, Ms. Djamshidi, about the importance of the public/private partnership, which I found very interesting. And I am wondering if the two of you could sort of share with us, maybe in priority order, what is the greatest concerns you have in dealing with the Federal Government, or dealing with the State or local government?

I am sure the problems are different, but if you could sort of tell us where you think the greatest concern would be for a small company trying to advance in the cybersecurity area, working with the Federal Government, what do you see are the major areas that we should be paying attention to, and then if you could, help our State our, the State of Maryland.

Ms. DJAMSHIDI. Sure. Did you want to take this?

Mr. IHEAGWARA. Ladies first.

Ms. DJAMSHIDI. Oh, okay. Sure. So in us working in a hands-on way with our companies, quite often we find these technology companies have dual purpose technologies. It applies in the area of cyber homeland security to the Federal space, but it also applies to various other commercial sectors.

So one of the key challenges that we try to work with our companies is essentially staying alive enough to be able to provide these innovations to the market. And so, quite often, that encompasses a number of activities. One is going after different markets; second is trying to help them get financed along the way, technology development takes capital; and in a very smart way, putting a capital strategy together is actually number one of the things that we work with our companies on that.

Senator CARDIN. But on capital, we are going through a very tough economic period.

Ms. DJAMSHIDI. Exactly, right.

Senator CARDIN. It is tough for anyone to get capital. Have you seen any of the tools that have been made available showing any improvement in the availability of capital?

Ms. DJAMSHIDI. I think so. I think I have seen some—it is definitely helpful, and with industry, we are lucky to have a DBED, we are lucky to have TEDCO. We have the MIPS program and various other programs that are available for financing the companies, and I think those are very helpful. Two of our companies most recently got TEDCO awards. That has been very helpful. We always work with our companies to try to look at all of these resources that are available.

But I have to say, there is still a lot more to be done. And so, we are sometimes having to go to Boston or go to California to get some companies financed. And so, more of that, I think, would be helpful. I think you also mentioned earlier that the capital to the companies, even though the banks say that they do have the capital, but they are not lending fast enough, is one of those key things that we are trying to tackle every day.

And we are trying to do everything we possibly can. For example, in the last two years, specifically it has been very difficult. One of the things that we have rolled into our services is aggressive business development for our companies. We are trying to get them faster and faster to their customers as a way of trying to bridge that gap. So we are trying to do everything that we possibly can to try to help expedite the companies so that companies do not fall sideways in the process as they are trying to bring some of these innovations out.

Senator CARDIN. Thank you. Dr. Iheagwara, you are to be congratulated, first, for being selected by DBED as Maryland Homeland Security Company of the Year, so I know you are going to say nice things about the State of Maryland. But could you perhaps tell us, in dealing with the Federal Government, what has been your greatest challenge?

Mr. IHEAGWARA. Thank you, Senator, for the congratulations and the good wishes. I have heard it two or three times today, so we are grateful that we won the award. But I must tell you that it has been a grueling fight. I am a fighter, generally speaking, and you cannot be a small business without being a good fighter.

The legislation, most of them are in place, but they have not been implemented, and where they are, not well-implemented. I listened to the testimony of Ms.—the lady from NSA, right? Talking about how easy it is to get 40 percent unclassified contracts, but that is not our experience.

We have attended the issues, we have registered. It is not easy. We tried very hard. We pushed. At some point, they requested for our capability statement. We went a step ahead by giving them our past performance record, which shows clearly in no unmistakable terms what we have done over 15 years, prime on eight Federal contracts and knocking out 20 other contracts with KPMG who was our mentor initially. That did not get any buy-in.

But we are on their database, and we keep receiving notices to attend and attend and attend. We are a small business. We do not have the resources. But look, here is the deal. We have proven that we can perform. We bid on contracts. It is difficult to win. The big boys are locked in. One is Xerox through the ACS, even in our State of Maryland here. I took issues with even Secretary—not Johansson—for Minority Affairs, Landau Jenkins.

I told her, we have submitted upwards of 50 solicitations to our own State of Maryland. We incorporated here 15 years ago. Not even a single contract from here. Yet, we have knocked out more than 20 contracts nationwide, all the way from Lines, Illinois to Honolulu, Hawaii for the U.S. Marine Corps, to Boston, Massachusetts for the U.S. Smithsonian, prime.

So you cannot tell us that we do not write good proposals or we do not have the past performance. So the animal we are dealing with here in Maryland is completely different. The Federal sector, the agencies there, is more about marketing money. We are a small business. It is not always to compete with IBM and all the big companies that have all the agents there deployed going after you.

Even as we speak now, if I give you a trajectory of our path, you will be impressed. I can tell you that, Senator. Look at it. So with eight Federal contracts, I state again, it is difficult for us to win.

So what they do, as you identified earlier on, is that they bundle all the contracts to add-ons and full-ons. Even when they advertise on bay for contracts, work, $25,000, the big boys will still compete and they will win.

So it is tough. So to sum it up, capitalization is very, very important for any small business. There are one of several ways to capitalize, one of which is the easy way, perhaps. Win contracts, hire new people, deploy them there, send money, and launch new initiatives, or you go for new markets or you go for venture markets, which is heavily tilted towards products and not services.

So I think capitalization is the toughest constraint, and if you can help us by making it a legislative mandate that all Federal dollars or State dollars, in the case of the State of Maryland, spent on cybersecurity, a certain percentage should go to small businesses, and, of course, request proof at the end of each fiscal year of delivery.

Senator CARDIN. That is good advice. I appreciate your suggestions and the points that you are highlighting are certainly ones that the Small Business Committee has made our top priority. So we are doing oversight hearings on that this year.

Ms. Djamshidi, let me ask you one additional question on this. Could you just share with me your observations of what the current budget situation has done in regards to these issues from two points of view? One, as we know, there has been reduced expectations as to what the Federal Government will be doing this year and the foreseeable future?

And number two, there is the unpredictability of whether we are going to have a shut-down, but whether we would have had a shutdown earlier this Congress or whether there was going to be a problem—whether we will have a problem on August 2nd paying any bills. What impact is that having on your work?

Ms. DJAMSHIDI. I tell you, it makes it more interesting and challenging at the same time. We feel that this whole circumstance that is going on, it hits us in multiple ways, and us I mean by the small businesses and us as an organization that represents the small business.

We find Federal agencies are quite often, a lot of the procurement vehicles are on hold, and so therefore, the buying decision has been dragged on for a longer period of time. And so, therefore, the small businesses are, therefore, affected.

And as we talked about, some of the vehicles for small businesses to get into some of the agencies quite often, because priming is very difficult, is to work in subcontract areas and to prove themselves by working with one of the system integrators. And there is a second wave of that.

The system integrators are, therefore, affected, and therefore, are not making those decisions and therefore, again, small business is affected by not being able to participate in some of those areas. So this delayed process is definitely affecting the companies. They still have to keep the lights on. They need to have revenues come through the door to pay for their employees, and it is very difficult to hold on to the employees in this current environment.

And so, it relates and it comes back to the small business in multiple ripples effects, and therefore, it makes it even more challenging. And I can provide more anecdotes.

Senator CARDIN. That would be helpful, thank you.

Dr. von Lehmen, could you respond also, too? The last three or four years have been tough years. Is it affecting the type of students that you are getting or their interest areas as they see the expectations, particularly at the Federal level of government, being diminished?

Dr. VON LEHMEN. The experience of institutions that serve working adults is that when the economy goes into a recession, enrollments pick up.

Senator CARDIN. Right.

Dr. VON LEHMEN. And that is because individuals are either out of work and seeking to recapitalize themselves through additional education or they still have a job but are concerned to maintain their positions by also getting additional education.

So what we have seen over the last three-plus years is actually growth from year to year in our student population. The majority of our students are in the programs that you would think they would be in. If you look at any college or university across the United States, it is typically business-related programs, programs that are related to information systems or computing, technology in general that experience the interest and the growth, and that has certainly been true for us.

And, of course, the leading example for us are our graduate programs in cybersecurity. Those programs were launched just last fall and are the cleanest measure of this growth. Today we have nearly 1,000 graduate students in those programs.

Senator CARDIN. Well, thank you. Again, let me thank this panel and thank all of those who were responsible for helping to put on this hearing here in Laurel. As I said in the beginning, this is a hearing of the Senate Committee on Small Business and Entrepreneurship. The information that has been obtained, the testimonies and the questioning, will be made available to all the members of our Committee and will be helpful in our role in oversight, as well as to try to plan appropriate policies to expand opportunities for small business.

Chairman Landrieu, Ranking Member Snowe, are both very much interested in these cybersecurity issues as it relates to business growth for small companies. And we are very interested in how the tools that we have already made available to deal with bundling—and we know the problems are there. Do not get me wrong. Our Committee is very focused on trying to deal with bundling abuses and, by the way, abuses between prime contractors and sub-contractors with the small business community.

We also are monitoring very closely the availability of credit through the mechanisms that were made available through the Small Business Jobs bill, and we will continue to monitor that. So your testimonies and the full record will be very helpful to the Committee, and I thank you all for participating.

The hearing record will remain open for two weeks for additional questions that could be asked by members of the Committee. In that case, if such are asked, we would ask that you try to get back

your answers as quickly as possible so that the Committee record will be completed in a timely way.

And with that, the Committee will stand adjourned. Thank you all very much.

[Whereupon, at 4:42 p.m., the hearing was adjourned.]

**Questions for the Record**

"The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States"

Monday, July 25, 2011

**The Honorable Patrick D. Gallagher, Director, National Institute of Standards and Technology, United States Department of Commerce**

**Question #1**

Mr. Gallagher, I was pleased to hear about the role small businesses play in supporting NIST.

- Could you describe for us the process your agency uses for acquisitions?

  **Answer** - NIST conducts acquisitions under "the Federal Acquisition Regulations System, which was established for the codification and publication of uniform policies and procedures for acquisition by all executive agencies." The Federal Acquisition Regulations System consists of the Federal Acquisition Regulation (FAR), which is the primary document, and agency acquisition regulations that implement or supplement the FAR. (FAR 1.101). Within the Department of Commerce (DOC), the Office of Acquisition Management establishes uniform policies for the DOC acquisition community, including NIST. The Department of Commerce's supplement is the Commerce Acquisition Regulation (CAR).

  NIST encourages the use of small businesses through a number of efforts, specifically including the NIST Small Business Specialist efforts to: (1) educate acquisition staff and end-users about our small business goals and small business programs and set-asides; (2) review procurement packages that are not intended for small business set-aside, and provide technical assistance to develop acquisition strategies and solicitation packages that are conducive to small business participation; (3) work with NIST organizational units to identify set-aside opportunities and create a accurate forecasts to enable small businesses to plan their efforts accordingly; (4) review procurement packages including the Statement of Work for each requirement over the Simplified Acquisition Threshold, and, when necessary, assist the Contract Specialist/Contracting Officer to ensure the requirement is written in a way that will allow small businesses to respond to all requirements; (5) support the efforts of the DOC Office of Small and Disadvantaged Business Utilization (OSDBU) and participate in multiple outreach events such as the annual OSDBU conference; and, (6) hold open house Industry Days (the next of which is on February 8, 2012) to allow small businesses to come to NIST to learn more about what we do, and the types of work that we will need contractor support to complete in the future.

- Specifically, if I were a small business, how would I secure a contract from NIST?

  **Answer** - NIST adheres to the FAR, and as such, appropriately advertises contracting opportunities. Small businesses are encouraged to participate and, when applicable, to compete to win contract awards. NIST does not maintain a qualified bidders list, or use any other prequalification methods; however, we reach out to small businesses to continue to broaden our supplier base. The Small Business Specialist (SBS) meets with small and small disadvantaged businesses to gather information and to counsel them on how to participate in and to pursue contracting opportunities. These meetings take place through large outreach events such as the OSDBU procurement conference, the Minority Enterprise Development conference, Industry Days, pre-proposal Conferences and site visits, Capability Demonstrations for 8(a) requirements, local industry-related groups and Chamber of Commerce events, other National conferences (Veteran's, Alliance events) and one-on-one meetings with individual small businesses that express an interest in serving the needs of NIST. The NIST Small Business Specialist is available to provide specific guidance to small businesses that want to compete for Federal contracts.

- Also, what percentage of your agency's contract dollars goes to small businesses?

  **Answer** - The NIST small business goal for FY11 was 46%, as set forth by the DOC OSDBU. At this time NIST believes it has exceeded this goal, ending the year with 66.3621% of contract dollars going to small businesses.

- How does the number for this year compare to previous years?

  **Answer** - NIST had a higher achievement in FY11 compared to the two previous years, which also exceeded the DOC goal. The total small business percentage was 58.0649% for FY10 and 59.9077% for FY09. NIST has consistently met or exceeded the goals set forth by the DOC.

- Also, do you have any additional plans to engage in Louisiana?

  **Answer** - As noted above, NIST participates in many small business-focused activities. Generally, these efforts are not state-specific. NIST welcomes participation from all states in these small business-focused activities.

**Questions for the Record**

"The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States"

Monday, July 25, 2011

**Jennifer S. Walsmith, National Security Agency Senior Acquisition Executive**

**Question #1**

Ms. Walsmith, you mentioned some of the Maryland-based partners with which the NSA has collaborated on cybersecurity.

- Have you worked with other organizations outside of Maryland on these issues?
- My state is also very interested in building our cyber capabilities and I want to support our technology innovators. Can you describe any initiatives you may have with organizations in Louisiana? What plans do you have to develop or expand collaboration with Louisiana entities?

**NSA RESPONSE**: There are 22 companies from Louisiana that have registered with NSA's Acquisition Resource Center (ARC). Of those 22 companies, 14 are small businesses. However, only one entity, Cyber Innovation Center, registered as a "cyber" company. During FY10 and FY11, we awarded contracts to 10 Louisiana entities. The contracts were in support of various research grants, as well as miscellaneous equipment and supplies.

In order to expand collaboration with Louisiana entities, NSA encourages direct contact with the NSA Office of Small Business Programs (OSBP) at (443) 479-2384. If there is enough interest, the OSBP can schedule a Pathways to Success meeting in Louisiana.

**Question #2**

NSA will be participating in a number of conferences this year, promoting opportunities for small businesses to compete for NSA contracts. One of the events you mentioned was the National Veterans Small Business Conference in New Orleans.

- Please tell us about this conference and what you hope to accomplish through your participation.

**NSA RESPONSE:** The National Veteran Small Business Conference and Expo brings together business owners and Federal Government representatives to share best practices of how to do business together. The conference features keynote speakers from Veteran's Affairs, the Department of Defense, and several other Agencies. The conference attracts close to 450 exhibitors and over 5,000 government and industry attendees annually. During the conference, NSA conducts a breakout session on how to do business with NSA, as well as participates in the Matchmaking Sessions to answer specific questions on how to best work with NSA.

The NSA Office of Small Business Programs attends this conference annually with the goal of broadening our industry base and reaching out to potential new vendors. We use conferences such as the National Veteran Small Business Conference as a mechanism to teach potential new business partners that working with NSA is not as daunting as it may seem.

**FOR THE RECORD**

**SENATOR MIKULSKI's QUESTION FROM DRAFT TESTIMONY (p. 45)** – Ms. Mikulski inquired as to the date when the next annual forum for unclassified companies will be held.

**NSA RESPONSE**: The annual forum held for unclassified companies has not been announced yet but is expected to be held in the April-June 2012 timeframe. Once arrangements are finalized, NSA's Office of Small Business Programs will contact Senator Mikulski's office with the details.

**Questions for the Record**

"The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States"

July 25, 2011

**Dr. Greg von Lehmen, University of Maryland University College**

Dr. von Lehmen, I commend your university for reaching out to other academic institutions in an effort to strengthen our cyber workforce. I am particularly excited about the agreement UMUC has with the Bossier Parish Community College.

- Please explain what the "two plus two" articulation agreement entails.

  **Answer**: Two plus two articulation agreements align the associate degree program at the community college to a corresponding bachelor degree program at UMUC to promote completion at both the community college and at the baccalaureate level. Programmatic articulation agreements are crucial to ensure successful transfer opportunities as it maximizes a community college student's time, money and credits by guaranteeing that their associate degree credits will transfer directly into a bachelor degree at UMUC, thereby minimizing student costs and time to completion. A program specific articulation provides a clear road map of what courses a student must take to earn their associate and bachelor degrees. Two plus two articulation agreements are an essential component of UMUC's national, comprehensive transfer program that consists of a series of interlocking programs and services to promote transfer success and credential completion.

- Also, do you have any additional plans to engage in Louisiana?

  **Answer**: At this time, we do not have any specific plans to engage further in Louisiana, but we are always looking to expand upon our relationships with community colleges and may do so in Louisiana the future. Representatives from UMUC currently visit Bossier Parish Community College once a month on a regular basis.

**Question for the Record**

**"The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States"**

**Monday, July 25, 2011**

**Sarah Djamshidi, Executive Director, Chesapeake Innovation Center (CIC)**

**Question**

Ms. Djamshidi, the Chesapeake Innovation Center serves as a bridge between public, private, and academic entities, all to promote the protection of our cyberspace and to develop the companies, technologies, and workforce to do so. I know several other states have similar establishments, such as the Cyber Innovation Center in Shreveport, Louisiana.

- Have you worked with any of these other organizations across state lines?

**Response**

In today's uncertain economy, innovative small businesses can hold the key to improvement and success. Organizations that facilitate public-private partnerships, such as the Chesapeake Innovation Center (CIC), in partnership with county, state and federal agencies, support small businesses and facilitate economic growth.

The Annapolis-based CIC is an initiative of the Anne Arundel Economic Development Corp. (AAEDC) and serves as a unique business incubator and accelerator. It is its direct connection between major users of technology and early-stage technology companies that are leading the way in innovation.

The CIC has developed a comprehensive plan to accelerate the growth of technology companies via unique programs in Anne Arundel County and in the region. Hands-on assistance and support, in addition to access to government and funding opportunities, are paramount in building a successful ecosystem where new innovative technologies, services and methods are born, supported and eventually deployed.

CIC has developed a number of programs to foster the entrepreneurship culture in the region. One of these programs is the Business-to-Government (B2G) CEO Roundtable, which is presented every other month. This program is designed to bring CEOs and company founders of emerging technology companies that serve the federal government (or those that would like to expand their business to the public sector) together to exchange information and dialogue on the issues that face small businesses.

Through TechBridge, a proprietary program of CIC, hundreds of companies have been screened, and more than 200 companies have come to Anne Arundel County to showcase their capabilities to the defense system integrators and federal agencies. To date, 48% of the companies participating in TechBridge came to the CIC from other states.

CIC is a member of the National Business Incubation Association (NBIA) and through this program and other initiatives, CIC reaches out to other incubators and accelerators across the country– and when appropriate and in partnership with those programs, CIC will showcase the emerging technology companies that meet the TechBridge Program requirements.

To date, CIC has not worked with the Cyber Innovation Center program in Louisiana, but has reached out to them and we hope to identify synergistic ways we can work together. We welcome collaborations with similar organizations – as it takes a robust network or an ecosystem of support to make significant contributions to the "Innovation Economy" and support the small businesses that are working hard to strengthen cybersecurity efforts.

MARYLAND
Department of Business & Economic Development

**Martin O'Malley** Governor
**Anthony G. Brown** Lt. Governor
**Christian S. Johansson** Secretary
**Dominick E. Murray** Deputy Secretary

August 8, 2011

The Honorable Benjamin L. Cardin
United States Senate
509 Hart Senate Office Building
Washington, DC, 20510

Dear Senator Cardin:

Thank you for convening the field hearing of the Senate Committee on Small Business & Entrepreneurship last week in Laurel. We appreciated the opportunity to update the committee on Maryland's cybersecurity initiatives and the role small businesses can play in defending the nation against cyber threats.

As a follow-up to the hearing, please note that Maryland plans to support small business efforts in cybersecurity in part by utilizing funds from the State Small Business Credit Initiative.

***How the SSBCI funds will be allocated***

Funds from the State Small Business Credit Initiative (SSBCI) totaling $23 million will be provided by the U.S. Treasury to the State of Maryland in three installments. The first installment of $7.5 million was received by the Maryland Department of Business and Economic Development (DBED) in June 2011. DBED is in the process of transferring these funds to four existing state program funds:

- Maryland Industrial Development Financing Authority (MIDFA) – $3.0 million
- Maryland Venture Fund (MVF) – $2.5 million
- Maryland Small Business Development Financing Authority (MSBDFA) Guaranty Fund Program – $1.5 million
- Neighborhood BusinessWorks – $0.5 million

Maryland DBED can request the second installment when it has demonstrated that it has utilized 80% of the initial installment.

***Promotion and outreach of financial assistance programs***

The DBED Office of Financing Programs regularly conducts outreach meetings with financial institutions around the state to familiarize lenders with DBED's financial assistance programs. DBED also holds similar meetings with the tri-county councils and county economic development offices.

The slowdown in lending activity over the past few years has prompted Maryland DBED to step up efforts to encourage banks to lend more to small businesses. In September 2010 DBED launched an initiative called "Credit Connections" to expand lending throughout the state by leveraging state and federal programs to increase the bankability of problematic loans. The Credit Connections initiative has focused on outreach to lenders on how to integrate multiple financing programs and meet challenging situations for borrowers. In less than a year the program has reached 55 Maryland lending institutions and over 200 lending officers.

This fall DBED will launch "Credit Connections 2" which will include:

- Adding a Credit Connections section to DBED's web site.
- Outreach to bank CEOs through a series of lunch meetings with the DBED Secretary. The first of these meetings is scheduled for October 2011.
- Additional workshops around the state to reach more lenders.
- Customized bank training sessions that pull together lenders from multiple divisions of the same institution at one location. Lender sessions are tentatively scheduled from January through May 2012.
- Incorporating the SSBCI funded programs into these workshops and presentations.

Marketing and outreach activities that will be developed specifically for the SSBCI funded programs include:

- A press/outreach strategy to include print and broadcast media. Identification of companies that are benefitting from the funding.
- Outlining message points and success stories for use by DBED's senior leadership to incorporate in to speeches, talking points, interviews and media releases when relevant.
- Creation of a "Frequently Asked Questions" on the four financing programs as a handout.
- Creation of a page on the www.choosemaryland.org web site specific to the SSBCI funded programs, as well as an ad linking it from the home page.
- Ongoing promotion through DBED's social media vehicles – blog, Twitter, *Pulse* e-newsletters – featuring businesses that have benefitted from the program.
- Hosting a webinar for lenders, businesses and stakeholders on how the program works and how to apply.

While the SSBCI funds add capacity to programs that can assist a wide variety of businesses, DBED hopes this added capacity – especially in the Maryland Venture Fund – will support aggressive initiatives for cybersecurity, information assurance and start-up technology companies who are part of the growing CyberMaryland infrastructure. A separate but complementary initiative involves connecting Maryland small businesses with federal procurement opportunities through the "Team Maryland Network" and the "Contract Connections" initiative.

***Developing the Cybersecurity industry in Maryland***

Since releasing *CyberMaryland* in 2010, Governor O'Malley has made cybersecurity an economic development priority. Working with the business community, colleges, research labs and federal facilities, DBED continues to lead efforts to position Maryland as the epicenter for information technology and innovation.

To market Maryland as the state for cybersecurity, DBED has undertaken a *CyberMaryland* brand marketing program. We unified cybersecurity marketing efforts under the CyberMaryland brand to demonstrate strength and enhance promotion. To date, a uniform logo, comprehensive web site (www.CyberMaryland.org), and aggressive social media marketing campaign have been launched. In August DBED will debut *CyberPulse*, an e-newsletter to regularly communicate news about this growing IT sector.

Maryland's strengths in cybersecurity have enabled three major industry-related conferences to recently be held in the state, most notably the C4ISR Joint Symposium and Expo at the Baltimore Convention Center in August 2010. DBED has actively participated in these and other such events around the country.

In the coming months we will launch new strategic advertising campaign in targeted markets and participate in a comprehensive outreach program of industry-based trade shows and conferences. A new exhibition will debut in August at the DISA Customer Partnership Conference, and will also be on display at the MilCom Conference in November – both at the Baltimore Convention Center.

***Improving Federal Procurement Opportunities for Small Business***

Team Maryland Network

In 2010, the Maryland Federal Facilities Advisory Board created the Team Maryland Network, compromising nearly 140 members representing small, medium and large companies conducting business with the federal government. About 75% of the members are from the IT, communications or cyber sectors. The Network's mission is to increase federal procurement expenditures with Maryland businesses and to foster cooperation among Maryland-based companies pursuing federal contracts.

Over 50 business leaders and sub-contractors participated in the first Team-Up Maryland event in May 2011, including representatives from Lockheed Martin, Northrop Grumman, Booz Allen Hamilton, CSC, ARINC, LMI, L-3, Raytheon and SAIC.

The next Team-Up Maryland event is scheduled for September 7 at the University of Maryland, Baltimore County. It will feature a series of five-minute presentations by 20 small and medium sized companies seeking to work with larger prime contractors.

Contract Connections

Contract Connections is a series of conferences and forums on federal government contracting that DBED undertook in 2010. These events also help small and minority firms directly connect with large contractors doing business with the federal government.

- Contract Connections Inaugural Conference, December 2010 – Thirteen federal agencies presented their contracting opportunities to 220 attendees. There were over 300 matchmaking sessions with these agencies.
- Contract Connections for Women, April 2011 – Offered a targeted seminar on a new SBA program for enhanced contracting opportunities for Women–Owned Small Businesses. Several agencies and a prime contractor presented business opportunities to 140 attendees.

The first two events filled up quickly and a third event is scheduled for December 2011. With a growing market for federal cybersecurity contracts, this initiative is perfectly positioned to help Maryland cyber companies connect with federal agencies.

We appreciate your continued leadership on this issue.

Sincerely,

Christian S. Johansson
Secretary

cc: Sen. Mary L. Landrieu, Chair, Committee on Small Business & Entrepreneurship

University of Maryland University College
*Office of the Provost*

11 AUG 10 PM 2:05

August 1, 2011

The Honorable Benjamin Cardin
United States Senate
509 Hart Senate Office Building
Washington, D.C. 20510

***Re:*** ***Committee on Small Business and Entrepreneurship Field Hearing – July 25, 2011***
***"The Role of Small Businesses in Strengthening Cybersecurity Efforts in the United States"***

Dear Senator Cardin:

Thank you for the opportunity to testify before the Committee on Small Business and Entrepreneurship on July 25, 2011. I hope my testimony on behalf of the University of Maryland University College (UMUC) was helpful to you and your colleagues.

In response to your request for more information on the demographics of UMUC's cybersecurity students, attached is information on students enrolled in UMUC's cybersecurity programs during the 2010-2011 academic year.

Thank you for your leadership on strengthening cybersecurity efforts and commitment to educating cybersecurity professionals in Maryland and throughout the United States. We look forward to working with you in the future. If you have any questions, please feel free to contact me.

Sincerely,

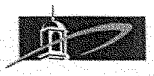
Greg von Lehmen

Greg von Lehmen, Ph.D.
Provost

Attachment

Cc: Members, Senate Committee on Small Business and Entrepreneurship

*3501 University Boulevard East, Adelphi, MD 20783-8001 USA*
*301-985-7174 • Fax 301-985-6432 • www.umuc.edu*



University of Maryland University College

**Cybersecurity Student Demographics**
**2010-2011 Academic Year**

| Racial/Ethnic Background | |
|---|---|
| American Indian or Alaska Native, non-Hispanic | 0.53% |
| Asian, non-Hispanic | 5.01% |
| Black or African American, non-Hispanic | 30.05% |
| Hispanic | 7.35% |
| Native Hawaiian or other Pacific Islander, non-Hispanic | 0.33% |
| Non-Resident Alien | 0.41% |
| Two or more races, non-Hispanic | 2.89% |
| Unknown | 9.04% |
| White, non-Hispanic | 44.18% |

| Gender | |
|---|---|
| Female | 27.00% |
| Male | 71.17% |
| Unknown | 1.83% |

| Age Range | |
|---|---|
| Under 25 | 12.95% |
| 25 to 34 | 44.06% |
| 35 to 44 | 26.22% |
| 45 to 54 | 13.76% |
| 55 to 64 | 2.81% |
| Over 65 | 0.20% |

| Military/Veteran Students | |
|---|---|
| Active Duty | 27.04% |
| Civilian | 2.28% |
| DoD Employee | 1.30% |
| National Guard | 1.14% |
| Non-Military | 48.86% |
| Reserve | 2.32% |
| Retired | 16.98% |
| Unknown | 0.08% |

| Military Branches Represented | |
|---|---|
| Air Force | 16.57% |
| Army | 16.16% |
| Coast Guard | 0.77% |
| Marine Corps | 3.66% |
| Navy | 13.15% |
| Non-Military | 48.86% |
| Unknown | 0.81% |

| Location of Students | |
|---|---|
| Asia | 2.57% |
| Europe | 10.83% |
| Baltimore | 22.11% |
| Norfolk | 2.20% |
| Salisbury | 0.29% |
| Washington, D.C. | 41.25% |
| Other locations | 18.69% |