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.