Statement before the US Senate Committee on Homeland Security and Governmental Affairs

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to our Nation's Critical Infrastructure"

Testimony of Elayne M. Starkey, CISSP, Chief Security Officer, Department of Technology and Information, State of Delaware

March 26, 2014

Good morning Senator Carper, Ranking Member Coburn, and members of the Committee. Thank you for inviting me to your hearing today.

As the Chief Security Officer for the State of Delaware, I can report that we are combatting a greater number of cyber-attacks than ever before. State governments not only host volumes of sensitive data about our citizens, we use the Internet to deliver vital services, and ensure our first responders can access the data they need in crisis situations. State government IT systems are a vital component of the nation's critical infrastructure.

Today, with this testimony, I want to provide the Committee information on the value of public-private partnerships. Cyber threats know no borders, and in our interconnected world where all levels of government work with each other, with private sector partners, and with citizens, the only defense is a multi-sector approach. I view these partnerships as a critical component of the Delaware Information Security Program and I am eager to give you specific examples of what is working in my state.

We have been partnering with the US Department of Homeland Security since our program started in 2004. Over the years, our incident response capabilities have improved significantly by participating in DHS's Cyber Storm Exercises. We have advanced our capabilities, thanks to applying funds from the Homeland Security Preparedness Grant Program to create government-wide programs that better secure our cyber infrastructure. We have used this money for annual employee

awareness training, e-mail phishing simulations, technical training, and exercises that test our ability to detect, respond and recover from a simulated large scale cyber-attack. I am grateful to receive approval for this funding. Delaware, however, is an exception. In contrast, most of my peers in other states report limited success in competing with traditional Emergency Responders for just a small share of the grant funds. I urge Congress to carve out a portion of this funding for states to use exclusively on cyber security initiatives.

One of the things I am most proud of is Delaware's effective outreach and collaboration with local governments and other critical infrastructure providers in the state. We were delighted to be selected to participate in the Community Cyber Security Maturity Model, run by the Center for Infrastructure Assurance and Security at the University of Texas at San Antonio. This program has resulted in training at all levels, exercises, seminars, and cyber conferences that are jointly planned and executed by the community. Our next event is a statewide cybersecurity conference on May 6. This is a day-long education workshop which will bring together state and local governments, law enforcement, military, higher education, healthcare, and other critical infrastructure providers. There is so much momentum here that the team has come together as the "Greater Wilmington Cybersecurity Working Group" and is active all year long.

Cyber Awareness, Education, and Training has been the cornerstone of Delaware's program since its inception. Our campaign is active throughout the year with newsletters, training sessions, and lunch 'n learn workshops. In October, as part of

National Cybersecurity Awareness Month, we ratchet up the program by adding many more education and awareness opportunities, employee scavenger hunts, TV and radio advertising, and even wrapping a Delaware Transit bus with an eye-popping cybersecurity message. This literally becomes a moving billboard, carrying the Internet Safety message to 50,000 motorists each day. And every year we offer an upbeat multi-media interactive presentation on Internet Safety to Delaware elementary schools. Thanks to an army of volunteers from my Department, other state agencies, Dover Air Force Base, and Verizon, we have reached over 25,000 fourth graders over the last 7 years. Verizon's support of this program has been unwavering. We could not have done many of these initiatives without the financial support from the Verizon Foundation and the incredible volunteer support from Verizon employees.

Cybersecurity works best when more people have an understanding of the risks and threats. I am especially appreciative of our strong partnership and collaboration with the Multi-State Information Sharing and Analysis Center (MS-ISAC), the National Association of Chief Information Officers (NASCIO), and FBI's InfraGard Program.

My final partnership example is with Higher Education. Five years ago, a team of people came together and discovered we all had a similar passion for attracting and nurturing the next generation of cybersecurity professionals. Today that team has evolved into a Coordinating Council that includes all Delaware Universities and Colleges. And together with the Council on Cybersecurity and SANS Institute, we

are planning our 5th annual summer US Cyber Challenge, a week-long, intensive camp filled with specialized security training intended to reduce the shortage in the cyber workforce.

This Saturday a select group of university students, returning veterans and job seekers will compete for the JP Morgan Chase Cyber Aces Governor's Cup. This program is intended to discover and develop talent and provide a pathway to cybersecurity careers.

Governor Markell is hoping to build on all these partnerships. In his January State of the State address, the Governor proposed building a collaborative research and learning network that leverages the public sector, academia, and the private sector. Delaware plans to locate the cyber initiative on the site of a former Chrysler assembly plant that is now owned by the University of Delaware and is already undergoing a transformation from car factory to Research Park. Ultimately, this will help build a skilled cyber workforce that will serve as a pipeline both for the State of Delaware and our businesses, and a hub for cyber innovation.

My complements to NIST and DHS and all of the stakeholders that worked together to develop the Cybersecurity Framework. It is valuable to state governments to reference a core set of activities to mitigate against attacks on our systems. For those of us that have established security programs, the Framework will not introduce major changes. Rather, the framework offers valuable risk management

guidance, and is complementary to our Exercise and Incident Response Program. It provides common language, sets a road map, and encourages continuous improvement. It also provides executive-level stakeholders with a succinct explanation of our cyber risk mitigation activities. I endorse the framework as an excellent first step; however, it is important to stress it is a BEGINING and not the END of a process. My hope is that future versions will include incentives to adopt the framework and strive for continuous reduction of cyber risk. I also believe NIST and other key federal agencies can work with states to build tools to assess and demonstrate compliance with standards and best practices. Both the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the National Association of State Chief Information Officers (NASCIO) are working with federal agencies to achieve these ends.

Cybersecurity is a complex issue, and we have a long road ahead of us to making our nation's systems more secure. It is a journey. It's a race with no finish line. There is no single solution, or a so-called "silver bullet". Holding hearings such as this one and finding ways to share information and resources will be crucial moving forward. I ask that Congress continue to work with the states to identify ways to protect our nation's information assets, and provide funding opportunities for state cybersecurity. Thank you.

Delaware Transit Cybersecurity Buses

4th Grade Internet Safety Presentation

Annual Delaware Cyber Exercise