Prepared Testimony and
Statement for the Record of

Ola Sage
Founder and CEO, e-Management
Co-Founder and CEO, CyberRx

Hearing on

"Oversight of the Cybersecurity Act of 2015"

Before the

Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies,
of the Committee on Homeland Security

June 15, 2016

311 Cannon House Building

Oversight of the Cybersecurity Act of 2015

Opening Remarks

Good morning Chairman Ratcliffe, Ranking Member Richmond, and distinguished members of the Committee. It is an honor for me to be here today.

My name is Ola Sage and I am the founder and CEO of two technology small businesses, e-Management and CyberRx, located in Silver Spring, Maryland. e-Management was founded in 1999 and employs nearly 70 information technology (IT) and cybersecurity professionals who deliver services in our core areas of IT Planning, Engineering, Application Development, and Cybersecurity. In 2013 e-Management was honored to receive the Department of Energy's Cybersecurity Innovative Technical Achievement Award, highlighting the capabilities of our cybersecurity experts in designing and implementing advanced cybersecurity detection and risk management capabilities. Earlier this year the U.S. Chamber of Commerce selected e-Management as one of the top 100 small businesses in America in 2016.

CyberRx, my second company, was launched in 2015 and offers a software platform that private sector companies, and small businesses in particular, use to help them measure, manage, and improve their cybersecurity readiness. Our software allows companies to quickly assess their cyber readiness and resilience using a unique application of the *Cybersecurity Framework (CSF)*, which was developed collaboratively with the *National Institute of Standards and Technology (NIST)*, academia, and industry. CyberRx is both vendor-agnostic and affordable, as we believe cybersecurity should be manageable and accessible to all organizations, particularly the most vulnerable—small- and medium-sized businesses (SMBs).

In April of this year, I was elected to serve as the chair of the *IT Sector Coordinating Council* (IT SCC). The IT SCC comprises the nation's top IT companies, professional services firms, and trade associations, and works in partnership with the Department of Homeland Security (DHS) to address strategies for mitigating cybersecurity threats and risks to our nation's critical infrastructure, especially for organizations and businesses that are particularly vulnerable, such as SMBs. One of the joint priorities this year with the IT SCC and DHS is to provide the SMB community with best practices and products for implementing the CSF to better protect businesses and manage risk.

I am also a nine-year member of Vistage, an international organization of more than 20,000 CEOs who control businesses that have annual sales ranging from $1 million to more than $1 billion. I regularly meet with and speak to small business CEOs in Vistage and other small business forums about why cybersecurity should matter to them and how it can affect their ability to keep business, stay in business, or get new business. Over the last 12 months alone, I have spoken to more than 200 SMB CEOs in a diverse mix of industries. I am a champion and advocate for SMB cybersecurity readiness.

Thank you for the opportunity to testify today as a small business owner.

In my testimony today, I will discuss:

- My company's experience with various government information sharing initiatives
- Perspectives on the *Cybersecurity Information Sharing Act* (CISA), and opportunities for the SMB community
- Concluding thoughts.

Experience with Government Information Sharing Initiatives

As an IT and cybersecurity small business provider, maintaining our competitiveness requires us to constantly add value to our clients by offering them the best combination of new products and services. In 2013, through our own research we became aware of the Enhanced Cybersecurity Services (ECS) program at DHS. ECS is a voluntary information sharing program that augments capabilities of critical infrastructure owners and operators by providing classified cyber threat "indicators" to improve protection of their systems and their customers. We reached out to learn more and were invited to establish a Memorandum of Agreement (MOA) to govern the government's provision and e-Management's receipt and use of information and ECS-related activities.

Following the execution of the MOA, we experienced our first hurdle. We knew ECS was a classified program and while we had a facility clearance, it was not at the level required to gain access to information needed to determine if we could participate in ECS. We spent weeks trying to locate a Sensitive Compartmented Information Facility (SCIF) that we could use just for a few hours to review the requirements to be an ECS partner. We reached out to various government contractors whom we knew either had a SCIF or access to one, but were turned down time after time. We eventually found a solution that enabled us to review the requirements, but to our disappointment, the financial barrier to entry was so high, we determined that it would be cost prohibitive for us to participate.

A year later, in 2014, we entered into a Cooperative Research and Development Agreement (CRADA) with DHS for an unclassified program that allowed DHS and e-Management to engage in data flow and analytical collaboration activities, including receiving relevant, unclassified, and actionable government-developed cybersecurity threat information. Through the CRADA, e-Management was also permitted to maintain access to or have an on-site presence within the National Cybersecurity and Communications Integration Center (NCCIC).

Our experience with the CRADA has been mixed. We do receive regular updates on threat information through the portal, which is very accessible; however, much of the unclassified information received is already widely available on the Internet or is dated, and therefore has limited use for our cybersecurity analysts or our clients. We ended up building our own Trusted Automated eXchange of Indicator Information (TAXII) server, pulling from open sources to collect threat information that we could use to better protect our company.

In 2015, we were informed of a new initiative called the Automated Indicator Sharing Initiative Dissemination Capability, which could enable us to participate in the dissemination of cyber threat indicators under the DHS Automated Indicator Sharing (AIS) Initiative TAXII server, in addition to the existing portal means provided through our CRADA. While we have an in interest in participating, establishing the necessary operational capabilities is constrained by limited resources.

An SMB CEO's Perspective on Opportunities for the CISA and Information Sharing Initiatives for Small Businesses

The Cybersecurity Act of 2015 provides a way for the government and the private sector to collaborate on cybersecurity while providing the necessary protections to alleviate the concerns of many companies, large or small, that they may be exposed to civil or criminal liability, reputational damage, or competitive threats. Some observations about the law, other information sharing initiatives, and some recommendations for how CISA can be more relevant to the SMB community, are as follows.

1. ***Small businesses are unaware of CISA.***
   CISA is new and though it applies to any size organization, today it is largely an interest of larger companies that have the infrastructure and resources to act. There is an opportunity for the government to increase the visibility of the law through its existing outreach and awareness programs to the SMB community through, for example, Small Business Administration (SBA) programs, or by working with Chambers of Commerce, small business associations, and trade groups.

2. ***Small businesses need to understand how CISA helps them.***
   In the law itself, there are only two references to small business, which highlights that this law is not directly focused on small businesses. How does CISA apply to SMBs in general? How does an SMB use CISA to help them better protect their business? Is CISA more applicable to certain types of small businesses? What protocols would help facilitate and promote the sharing of cyber threat indicators with the SMB community? Answers to these and other questions would help clarify the law's applicability to SMBs.

3. ***Small businesses are confused by the myriad of information sharing initiatives.***
   The number and variety of information sharing initiatives is overwhelming to many small businesses, if they are even aware they exist. For example, Enhanced Cybersecurity Services, the Cooperative Research and Development Agreement, the National Cybersecurity and Communications Integration Center, Automated Indicator Sharing, the Information Sharing and Analysis Centers, and/or the Information Sharing and Analysis Organizations, are just a few of the information sharing initiatives companies can participate in. It would be helpful to the SMB community if these initiatives could be streamlined and tailored for the SMB community.

4. ***Cybersecurity is costly for small businesses.***
   Implementing cybersecurity best practices and solutions is costly for many small businesses. Some industry estimates suggest costs of up to $60,000 a year for a 50-employee company, and it is not clear to many what the concrete benefits are of investing those kinds of dollars in cybersecurity. As information sharing is voluntary under the law, the key driver for a small business CEO to consider participation will be the cost to implement. There is still a significant percentage of small businesses owners who do not believe that they have anything that criminals would want. It would be helpful if there could be an estimate, on average, of what it would cost a small business to participate in the information sharing forum (*e.g.*, similar to the time estimates that are provided for completing government forms).

Conclusion

CISA is in its early stages and we recognize that over time the implementation of the law will mature providing more clarity for its application, particularly for SMBs. We at e-Management and CyberRx are committed to working with government and industry to identify and promote affordable solutions that enable small businesses to strengthen their cybersecurity readiness and posture.

Thank you again for the opportunity to testify. I am ready to answer any questions you may have.