Opening Statement
Chairman Steve Chabot House Committee on Small Business Hearing:
"Small Business Cybersecurity: Federal Resources and Coordination"

March 8, 2017

Good morning. I call this hearing to order. Thank you all for being here today.

Over the past year, this Committee has turned its attention to an issue that is increasingly serious for small businesses: cybersecurity. In past hearings, we heard firsthand accounts from small business owners who have been the victims of cyber attacks.

We have also heard dire warnings from cybersecurity experts about the new and varied cyber threats facing America's 28 million small businesses.

There is no question that advances in information technology have helped small businesses to increase their productivity, become more efficient, and ultimately, more successful.

However, the same tools and resources that have given small business owners a greater role in the marketplace have also provided cyber criminals and foreign bad actors with more opportunities to steal sensitive and valuable information that small businesses rely on to remain competitive.

In 2015 alone, the United States Department of Justice recorded nearly 300,000 cybersecurity complaints.

We have also learned that a cyber attack can have serious consequences, not only for small businesses, but also their customers, employees, and business partners. Sixty percent of small businesses that fall victim to a cyber attack close up shop within six months. A 2014 survey from the National Small Business Association estimated the average cost of a cyber attack on a small business to be over $32,000.

In our Committee's efforts to spotlight these serious and growing threats, it has been abundantly clear that the federal government needs to step up its game when it comes to protecting the cybersecurity of small businesses and individuals. And, to some extent, federal agencies have begun offering resources directly to small businesses in recent years.

Today we will hear from some of the federal agencies that are already providing cybersecurity resources to small businesses. We will examine how these tools can be more easily accessed by small business owners and ensure that they are effective.

Since the late 90s the federal government has become increasingly active in protecting our nation's critical infrastructure and information technology (or IT) systems. It has gone to great lengths to coordinate these efforts with state and local governments, as well as the private sector. However, it wasn't until recently that the federal government was encouraged to engage in greater information sharing practices with businesses through the development of an overall framework for cybersecurity protocol. The framework would enable businesses of all sizes to implement a set of best practices for assessing cyber threats and reinforce their cybersecurity systems.

Just last year, the House passed the Improving Small Business Cyber Security Act, a bill that helps small businesses facing cyber threats by providing access to additional tools and resources through existing federal cyber resources. The bill became law as part of the National Defense Authorization Act of 2017. The Department of Homeland Security (DHS) and other federal agencies have been permitted to work through Small Business Development Centers (or SBDCs) to streamline cyber support and resources for small businesses.

While I believe this is a great start, I think it is glaringly obvious, that federal agencies tasked with providing small businesses with cybersecurity resources to small businesses can be even better coordinated. They should drive down duplicative resources and processes and ensure that small businesses are equipped to deal with the growing cyber threats. I look forward to hearing our witnesses' views on how we can more efficiently disseminate federal cybersecurity resources to America's small businesses.

I now yield to the Ranking Member for her opening statement.