OPENING STATEMENT
AS PREPARED FOR DELIVERY

SMALL BUSINESS COMMITTEE

Opening Statement of Chairman Steve Chabot

House Committee on Small Business Hearing:

"Foreign Cyber Threats: Small Business, Big Target"

AS PREPARED FOR DELIVERY

July 6, 2016

Good afternoon and thank you all for being here today. A special thank you to all of our witnesses for coming here to share their expertise and experience.

Small business cybersecurity has been a top priority for our Committee throughout this Congress. In our previous hearings, we have heard stories from small business owners who have been the victims of cyberattacks. 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 doubt that the Information Technology (or IT) revolution has provided small businesses with new tools and opportunities to compete in the global economy.

However, we must be mindful that as small businesses use this technology, the risk of a foreign cyber-attack has increased dramatically.

According to a recent report by Verizon Enterprise, a shocking 71 percent of cyber-attacks occurred in businesses with fewer than 100 employees. As we have heard many times, even one cyber-attack can be devastating for a small business, making prevention and protection absolutely critical. 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.

Our committee's efforts to spotlight these serious and growing threats have made it abundantly clear that the federal government needs to step up its game when it comes to protecting the cybersecurity of small businesses and individuals.

Today's hearing will examine the increased threats posed by foreign actors to American small businesses in cyberspace. This is an important dimension of the cybersecurity threat that impacts both our national security and our economic security and I believe it demands much more attention than it has received so far.

The Federal Bureau of Investigation has already determined that foreign state actors pose a serious cyber threat to the telecommunications supply chain. It is also clear that many foreign nations are responsible for direct cyber attacks on the United States in an effort to steal intellectual property and sensitive personal information.

The Office of the National Counter Intelligence Executive released a report in 2011 stating that tens of billions of dollars in trade secrets, intellectual property, and technology are being stolen each year from computer systems in the federal government, corporations, and academic institutions. China and Russia were cited as the two largest participants in cyber espionage.

In a report by our colleagues on the House Permanent Select Committee on Intelligence, U.S. businesses and cyber security experts have reported persistent attacks that could be traced back to China and were thought to be supported by the Chinese government. And, studies from the Department of Defense have warned of the difficulties associated with defending against threats posed by foreign nations, stating, "means and opportunity are present throughout the supply chain and lifecycle of software development."

This is particularly troublesome for small businesses that, not only rely on products from, but also engage in commerce with, globalized telecommunications firms from countries like China.

Small businesses play an indispensable role in providing the federal government with products and services. They are integral links in the government supply chain but are often ill-equipped to combat against sophisticated foreign cyber-attacks. This makes them a prime target for state sponsors of cyber terrorism who wish to undermine America's commerce and security.

I look forward to hearing our witnesses' assessment of this threat as well as their suggestions for how we may better guard against it.

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