House Committee on Small Business
Small Business Information Sharing: Combating Foreign Cyber Threats
Opening Statement—As Prepared for Delivery
Chairman Steve Chabot

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

Over the past few years, this Committee has focused its attention on an issue that has become increasingly important for small businesses: cybersecurity. In past hearings, we have learned that a cyber attack on a small business can have serious consequences, not only for the business itself, but for its customers, employees, and business partners alike.

We have heard from small business owners, cybersecurity experts, and government officials, and there is no question that improving cybersecurity for America's small businesses should continue to be a top priority.

In today's global economy, small businesses are increasingly turning to foreign technology to remain competitive in the world marketplace. However, these same products and services also provide new opportunities for foreign cyber criminals to infiltrate small business information technology systems, allowing them access to sensitive and valuable information.

A recent survey found that 81 percent of small businesses are concerned about a cyber attack, but only 63 percent have the most basic cybersecurity measures in place to combat such an attack. Cyber attacks pose a higher risk for small businesses since most do not have the means to hire specialized employees or pay the average $32,000 in damages. And, cyber threats for small businesses are on the rise.

This Committee has also found that the federal government is stepping up its efforts to both prevent and mitigate cyber attacks by coordinating and distributing cybersecurity resources directly to small businesses. There is strong bipartisan support from both chambers of Congress and the President to increase American protection from foreign cyber attacks.

However, small businesses are still hesitant to engage with the federal government. This is often due to uncertainty surrounding legal liabilities, concerns about privacy and data protection, and a number of other factors. Still, federal information sharing is crucial to ensuring that small businesses have every resource possible to combat cyber threats and the confidence they need to engage with the federal agencies tasked with protecting them.

That is why the Ranking Member and I recently introduced H.R. 4668, the Small Business Advanced Cybersecurity Enhancements Act of 2017, to increase the defensive measures available for small businesses undergoing or concerned about a cyber attack and to incentivize additional information sharing between private sector and the federal government.

This bipartisan legislation seeks to safeguard small businesses from cyber attacks in a few simple ways. First, the bill establishes Small Business Development Centers, or SBDCs, as the primary liaison for federal information sharing for small businesses. This bill also ensures that small businesses that engage with SBDCs receive the same protections and exemptions provided by the Cybersecurity Information Sharing Act, or CISA.

Further, this bill would ensure that any policies or rulemaking adopted by any federal agency as a result of federal information sharing does not unfairly burden small businesses. It would also expand liability protections for small businesses that engage with the federal government in good faith. Ultimately, this legislation removes the barriers many small business owners face when confronted with a cyber threat, encouraging them to work with the federal government; not fear it.

As I mentioned before, many cyber threats towards small businesses come at the hands of foreign bad actors, sometimes foreign governments, in an attempt to undermine the United States' national security and economy. In fact, the Department of Homeland Security recently published a public notice exposing a vulnerability in a notable security camera company.

Hikvision [HIKE-vision], one of the top 5 largest manufacturers of security cameras worldwide, is 42% owned by the Chinese government and, in 2017, DHS learned that many of its cameras were able to be hacked and remotely controlled. While Hikvision has worked with DHS to remedy the flaw, the problem remains that many small businesses that do not engage with the government or DHS regularly may not be aware of the security flaw. Had the problem gone unnoticed, many small businesses would not have known that they were vulnerable to attack.

So, I look forward to hearing from our witnesses today to learn more about how the federal government is working to address these important problems, and further, what preventative measures small businesses can use to protect themselves from falling victim from cyber attacks.

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