OPENING STATEMENT
AS PREPARED FOR DELIVERY

SMALL BUSINESS COMMITTEE

Opening Statement of
Chairman Steve Chabot
House Committee on Small Business
Hearing: "Small Business and the Federal Government: How Cyber-Attacks Threaten Both"
AS PREPARED FOR DELIVERY
April 20, 2016

Good morning and thank you all for being here today. And thank you to all our witnesses for coming here to share their insights and expertise with this Committee on a very timely and very important subject. In April of last year, this Committee heard from a panel of industry experts about how small businesses across the country are being threatened by a growing number and variety of cyber-attacks. Since then, the threat to small businesses has only grown. Unfortunately, in many ways, the federal government's efforts to guard against this threat have not kept pace.

This morning, the Committee will look at the effects of cyber-terrorism and cyber-attacks on both small businesses and the Federal Government. Small businesses face an increased risk because they lack the resources to protect themselves against sophisticated cyber-attacks. We must make sure that the federal government is part of the solution and not adding to the problem. It is vital to both the economic and national security of the United States that the sensitive data held by the Federal Government be safeguarded. The owners, employees and customers of America's 28 million small businesses need to have confidence that their data is secure.

I think it is fair to say that confidence has been shaken in recent years with the cyber-attacks on the IRS, the State Department, OPM, and even the White House. Between foreign hackers from countries like China and Russia and domestic identity thieves, the federal government has a target on its back that seems to get larger by the day.

This is why recent findings from the Government Accountability Office (GAO) on cybersecurity problems at agencies like the IRS and the SBA are so troubling to me.

Just this month, GAO reported that the IRS paid 3.1 billion dollars in fraudulent Identity Theft (or IDT) tax returns. When GAO testified before this Committee earlier this year, they told us that "the SBA has not conducted regular reviews of its IT investments." In these scenarios, American small businesses and consumers were put at risk due to a lack of diligence by Federal Agencies. Just last week, I asked IRS Commissioner about the data breach at his agency last May which exposed the data from approximately 700,000 accounts. The Commissioner informed our Committee that there are one million cyberattacks at the IRS every day. With over 3 billion different mobile applications and 340 billion dollars in online commerce sales last year, business transactions are moving away from the cash register and toward the smart phone. It's great to be able to order your coffee, pay your electric bill, or reserve a car ride using your phone. But with this convenience comes increased exposure for both the customer and the business. In 2015 the average amount stolen from small business bank accounts after a cyber-attack was over 32,000 dollars.

The fast pace of changes in technology means that hackers are coming up with more sophisticated methods to go after intellectual property, bank accounts, Social Security numbers, and anything else that can be used for financial gain or a competitive edge. With all of the uncertainty facing small businesses in today's world of e-commerce, it will take vigilance by all federal agencies and the watchful eye of this Committee to ensure the data of small businesses and individual Americans remains secure. We must also look for new and innovative ways to help small businesses protect their data from this great and growing threat.

I look forward to hearing from our witnesses and I now yield to the Ranking Member.