**Statement of Ranking Member Thomas R. Carper**
*"The IRS Data Breach: Steps to Protect Americans' Personal Information"*
June 2, 2015

*As prepared for delivery:*

Nearly every day, we learn of another major cyber attack or data breach on an American company or organization. In many ways, we are dealing with an epidemic of online theft and fraud. That epidemic is growing at an alarming rate and continues to victimize and frustrate more and more of us.

Over the past several months, for example, we witnessed several companies in the healthcare sector suffer major data breaches. And, of course, we know that our government networks are under constant attack in cyberspace.

These attacks are growing ever more sophisticated, too. That's happening at least in part because our defenses are also getting better. Still, we must do more to stay ahead of those that would do us harm. And, we must learn from those instances when criminals have been successful in getting past the protections we put into place and create havoc.

Today, we will take a closer look at the recent cyber attack on the Internal Revenue Service (IRS). We will examine what went wrong, how the IRS is trying to repair the damage, and what we can do to reduce the likelihood to make sure that something like this doesn't happen again, either at the IRS or elsewhere.

From what we know so far, the attack on the IRS appears to have been an especially sophisticated one. We also know that the IRS had defenses and fraud prevention measures in place at the time of the attack. Yet despite the precautions that were taken, skilled criminals were able to use innovative tactics to trick the IRS system into releasing past tax returns.

Given the vast amounts of sensitive information the IRS possesses, it is critical that the agency continues to do more to protect the American taxpayer. In fact, all agencies need to step up their efforts and improve their cybersecurity posture. The wake-up call has been ringing for years now. We need an all-hands-on deck effort in responding to it.

As we know, cybersecurity is a shared responsibility. Those of us here in Congress have an obligation to ensure that agencies have the funding, the tools and the authority they need to adequately protect their systems from attack. Unfortunately, Congress has significantly reduced IRS funding in recent years, and we've done so while also tasking the agency with far greater responsibilities. In fact, the IRS is operating at its lowest level of funding since Fiscal Year 2008. These cuts have had real consequences for the agency and American taxpayers.

I look forward to hearing from the Commissioner today about what he needs to better protect his agency from fraud and cyber attacks. Here in the Committee, we've been working hard to address our country's cybersecurity challenges. Our efforts led last year to the enactment of four key pieces of cybersecurity legislation. One of these bills updated the Federal Information

Security Management Act or 'FISMA' to better protect federal agencies from cyber attacks. Another codified the DHS cyber operations center. The two others strengthened the cyber workforce at the Department of Homeland Security.

This year, I introduced an information sharing bill and have been working closely on this issue with our colleagues on the Senate Intelligence Committee. I have also been working closely with Senator Blunt on data breach legislation that will create a national standard for how we protect data and consumers. It is my hope that we can come together as a Congress to pass these two important pieces of legislation and provide our agencies with the resources they need to tackle the nation's growing cyber threat. With that, I would like to thank all of our witnesses for joining us here today. We look forward to your testimony.

###