Statement of Ranking Member Thomas R. Carper

"Under Attack: Federal Cybersecurity and the OPM Data Breach"

June 25, 2015

As prepared for delivery:

Thank you, Mr. Chairman, for calling this very timely hearing. And welcome to all of our witnesses.

A few weeks ago, we learned of a massive data breach at the Office of Personnel Management (OPM). Personal and financial information for more than four million current and former federal employees may have been compromised. As if that was not bad enough, reports now indicate that background investigation information - some of the most sensitive personal information the federal government holds – may also have been compromised, potentially touching millions of additional individuals.

This attack is deeply troubling and could have far-reaching consequences for a great number of people. It could have a profound impact on our national security, as well.

Understandably, the public and my colleagues are upset, and they are frustrated. They want answers. So do I, and so does this Committee. Before we leave here today, I want us to learn the answers to at least four questions: First, what went wrong? Second, what are we doing about it? Third, what more needs to be done? And, fourth, how can Congress help?

Ultimately, sustained corrective action will be needed before we restore the public's confidence in our government's ability to keep their personal information safe and secure.

I was encouraged to hear that OMB recently launched a 30-day "cybersecurity sprint" to further protect federal systems from cyber attacks. This is a good start, but I think we can all agree it's not enough.

As we can see from OMB's most recent annual report card on federal network security, there is much room for improvement. It should be the goal of every agency – large and small – to be at the top of this table. Having said that, making it to the top of this chart does not guarantee immunity from a successful cyber attack. Too many of the bad guys are good at what they do, and they're getting better all the time. We've got to bring our 'A' game to this fight every day. It's all hands on deck all the time.

For those agencies that continue to lag behind, there needs to be enlightened leadership, accountability and a commitment to continuing improvements.

One valuable cybersecurity tool that is available to all federal agencies is a Department of Homeland Security (DHS) program known as EINSTEIN. It is not a panacea. It is a system that can record, detect, and block cyber threats.

All of us on this committee have recently heard about the importance of EINSTEIN after the OPM breach. This system used cyber threat information from the OPM data breach to uncover a similar intrusion – which we may have never known about – at the Department of Interior. That

was an important discovery. But finding out about data breaches after they occur isn't good enough. We want to be able to stop these attacks before they can do any damage.

It is my understanding that the newest version of EINSTEIN – EINSTEIN 3A – can do just that. Unfortunately, today, less than half of all federal civilian agencies fall under the protection of EINSTEIN's most advanced capabilities.

I recognize this system is not perfect – no system is. But, as my colleagues and our staffs have heard me say many times, if it isn't perfect, make it better. From everything I've heard, EINSTEIN 3A is another important and badly needed step toward that goal.

And that is exactly why Senator Johnson and I – along with our staff members – are working on legislation now to authorize and improve EINSTEIN. This legislation would speed up its adoption across the government, require use of leading technologies, and improve accountability and oversight.

I look forward to working with my colleagues on this legislation so that we can ensure every agency is equipped with the ever-improving capabilities needed to fend off cyber attacks in the future. In closing, I think it's important to recognize the breach at OPM follows a long list of major cyber attacks against the government, as well as the private sector. And, there is likely more to come.

To tackle a challenge this big, we need an 'all hands on deck' approach. What does this mean? Simple, we need all the people, resources, and authorities we can reasonably muster to be at the ready to respond.

We could begin by continuing to help fill top spots in our government agencies, something at which this committee has largely done a superb job. OPM, for example, has been without a Senate confirmed Deputy Director for nearly four years. It's not that the Administration hasn't been submitting the names of qualified and talented candidates for these posts most of the time. For example, this Committee has favorably reported out the name of Navy Admiral Earl Gray, the President's nominee for this position, twice— once in 2014 and again in 2015. We need to get him confirmed so Director Archuleta has the help she needs to right the ship.

We could also build on the cyber legislation we passed last year or pass new legislation like EINSTEIN, information sharing, or data breach. We could also fully fund agency security efforts.

These are all important steps we can take, but they will incredibly difficult to accomplish if we don't work together. With that, Mr. Chairman, I thank you again for holding this hearing. I look forward to hearing from our witnesses.

###