Opening Statement of Ranking Member Tom Coburn

"Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure"
March 26, 2014

As prepared for delivery:

Cyber threats are one of the most serious national security threats facing our nation. Nation-states and other adversaries continue to commit or condone cyber espionage against our businesses and citizens — stealing our intellectual property and sensitive business information. Some have called these attacks the greatest transfer of wealth in human history and one of the significant headwinds facing our economy. Cyber-crime is also a growing and serious problem — imposing significant costs on our citizens and our economy. I remain concerned about the potential acts of cyber-sabotage or terrorism against our nation's critical infrastructure from those who wish to do us physical harm and disrupt our way of life. How to address and mitigate these threats will be one of the biggest challenges facing our nation in the years ahead.

I appreciate the hard work of the officials at the National Institute for Science and Technology (NIST) and the Department of Homeland Security (DHS). Their dedication to public service is uplifting. Ms. Dodson, I applaud NIST for the good job you did developing the Cybersecurity Framework. You worked with the private sector, listened to their ideas, and developed a workable, flexible process that can have significant positive impact in the private sector.

Dr. Schneck, I am interested to hear more from you about the DHS's plans for working with the private sector and states to help them use this tool, as well as your plans to encourage its adoption. I am also interested to hear your plans to encourage better information sharing from and between government and the private sector. Information sharing is most important partnership we can form to help our businesses better defend their own networks.

More clarity is needed regarding the ultimate goal of Executive Order 13636 though; it should not be federal regulation of cybersecurity. The last thing that we need is a top-down regulatory model for cybersecurity. Let's be clear — Washington does not have all of the answers for cybersecurity. Even if it did, the Federal Government would struggle to manage or enforce rules for good cybersecurity practices. Each computer network is unique and computer networks are not well-suited to the inflexible, prescriptive, check-the-box approach of a regulatory regime. I worry that a mandatory cybersecurity framework would harm cybersecurity more than it helps — shifting resources from dealing with actual cybersecurity risk to regulatory compliance.

Consider the Federal Government's poor track record of securing its own networks. As I revealed in my report last month — *The Federal Government's Track Record on Cybersecurity and Critical Infrastructure*, which I will include in the record for this hearing — many agencies are still failing to practice the basic cyber hygiene necessary to protect their computer networks and systems. Even the Department of Homeland Security has trouble securing its networks. For example, DHS is one of several federal departments and agencies that continues to run Windows XP on some computers, which Microsoft will stop issuing patches and software updates for early

next month. Systems running Windows XP will become ripe targets for hackers once Microsoft stops supporting those systems. It is simply irresponsible to run such unsecure operating systems on critical systems and government networks.

With the Federal Government unable to maintain its own cybersecurity, why should the private sector trust it to be a competent manager or regulator? Let me quote the November 2013 report of the *President's Council of Advisors on Science and Technology*, which was prepared by some of our top experts in science and technology and released by the White House:

> *The Federal Government rarely follows accepted best practices. It needs to lead by example and accelerate its effort to make routine cyber-attacks more difficult by implementing best practices for its own systems.*[1]

The Council's first recommendation was to phase out the use of unsupported and insecure operating systems, such as Windows XP, in favor of modern systems within two years. If the Federal Government is to be a trusted and effective partner in cybersecurity, we need to lead by example and get our own house in order first.

We also need to do a better job with our programs working with the private sector. I am pleased to have Mr. Stephen Caldwell here from GAO to testify today. He will review the Department of Homeland Security's track record working with critical infrastructure sectors. Too often the Department has struggled to implement programs like the Chemical Facility Anti-Terrorism Standards (CFATS) program and information sharing with the private sector. My hope is that DHS experts will learn from their past mistakes and GAO's analyses to become more successful in rolling out programs through better consultation with the private sector.

We also need to question whether the Federal Government's current approach to cybersecurity is the right one. Rather than just focusing on vulnerability mitigation — putting more locks on the doors to our networks — we need to be thinking about deterrence — disincentivizing bad actors from trying to break through those doors in the first place. A determined adversary like a nation state is going to be able to get into our networks regardless of our defenses. As Suzanne Spaulding, who now leads federal cybersecurity programs like Einstein and Continuous Diagnostics and Mitigation as DHS's Under Secretary for National Protection and Programs, once wrote, "The promise of an impervious cybersecurity shield protecting vast amounts of information from a determined and sophisticated adversary is at best a distant dream, and at worst a dangerous myth."[2] I agree.

We need to be changing the cost benefit analysis of our adversaries, so they think twice about whether attacking our networks. There is bipartisan interest, including from some members on this Committee in applying deterrence as a strategy through bills like the Deter Cyber Theft Act. I am pleased to have Mr. Steve Chabinsky — formerly of the FBI — here with us today on our

---

[1] EXECUTIVE OFFICE OF THE PRESIDENT, PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, REPORT TO THE PRESIDENT: IMMEDIATE OPPORTUNITIES FOR STRENGTHENING THE NATION'S CYBERSECURITY (November 2013), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_cybersecurity_nov-2013.pdf.

[2] Suzanne E. Spaulding, *No More Secrets: Then What?*, THE BLOG, HUFFINGTON POST (June 24, 2010, 10:55), http://www.huffingtonpost.com/suzanne-e-spaulding/no-more-secrets-then-what_b_623997.html.

second panel. He has been on the front lines of the cyber fight since the 1990s and can speak to this issue, whether we are following the right strategy, and what more can be done.

In closing, there is no question that cybersecurity is an increasing problem for our nation, and it is only getting worse. It is also true that when Congress tries to write big bills, they often go nowhere; or worse, they pass and only exacerbate the nation's problems. One area where I do think we can focus is fixing cybersecurity within the Federal Government. If the Federal Government is to be an effective and respected partner with the private sector, it needs to start with improving its own cybersecurity.

I thank you and look forward to your testimonies.