Opening Statement of Sen. Tom Coburn, MD
Ranking Member
Homeland Security and Governmental Affairs Committee
Hearing on Data Breaches
April 2, 2014

Welcome, Sen. Blunt, and all of our witnesses here today. I would particularly like to thank Mr. Greg Wilshusen from GAO for appearing as the minority witness to discuss the federal government's challenges with cyber security and data breaches.

Data breach incidents are a serious problem. When we see examples like the Target data breach, with millions of people's personal information exposed, it is clear that our businesses need to do a better job protecting their customers' information.

I am open to legislation that would streamline data breach rules. However, we need to be careful to not be too prescriptive or punitive against companies. I look forward to learning more about Sen. Carper and Sen. Blunt's bill today.

We shouldn't lose sight of our responsibility to oversee the Federal government's data protection efforts. This Committee has clear jurisdiction over federal cyber security. I would like to take this opportunity to formally request that the next hearing this Committee holds on cyber security focus on federal cyber security and whether agencies are doing all they can to protect our sensitive information.

The American people don't have a choice but to give the Federal government their information. They don't have a choice but to submit their tax records every year to the IRS. They don't have a choice but to participate in the Social Security system. And now many don't have a choice but to sign up for HealthCare.gov. That data is no more secure in the federal government than in the private sector, and probably less so, in many cases.

Just as Target and other companies have a responsibility to protect their customers' information, the Federal government has a responsibility to protect the sensitive information it manages.

Too often, the Federal government fails to practice good cyber security.

Consider some examples: Last July, hackers stole the private information of 100,000 people from the Department of Energy. In 2012, the Thrift Savings Plan experienced a data breach that jeopardized 123,000 of their account holders' information. And earlier this year, the Department of Homeland Security exposed financial information and private documents that belonged to organizations that were bidding for contracts with the DHS Science and Technology (S&T) Directorate.

OMB and the Department of Homeland Security need to do a better job managing Federal cyber security. The GAO has done good work auditing federal cyber security, and identifying the many challenges that we face. I am happy that Mr. Wilshusen of GAO can join us today to speak to these problems and how we can fix them.

The Department of Homeland Security also needs to do a better job with its programs for Federal cyber security. Just today, the DHS Office of Inspector General released an important report looking at DHS's Einstein program.

Einstein is supposed to be the federal government's intrusion and prevention system for federal agencies. The DHS OIG identified a number of problems, including that the Department is not adequately monitoring the program's implementation and its handling of personally identifiable information.

The Inspector General reported: "There is little assurance that NPPD would be able to deliver intrusion prevention capabilities to participating agencies on

schedule." This is a key system that DHS views as the solution to protecting federal networks, and apparently it is not being managed effectively.

We also need to ask whether we are focusing on the right priorities for our cyber security spending. I welcome Mr. Noonan from the Secret Service today, and I look forward to his testimony. I am interested to know just how many resources we have devoted to investigating cyber crime and arresting the criminals who are stealing our information.

I am concerned we are spending most of the federal cyber security resources at DHS on vulnerability mitigation, and just a fraction on US Secret Service and FBI agents who are catching cyber criminals. Investigating and arresting cyber criminals is one of the best ways that we can deter cyber crime and protect our information.

We need to focus more on that kind of deterrence.