STATEMENT OF SENATOR TOM COBURN

Chairman, Subcommittee on Federal Financial Management, Government Information and International Security

July 19, 2005

On the morning of April 19, 1995, Oklahoma learned firsthand the horrific effects of terrorism in the homeland. The prevention of terrorism starts with a proactive plan with cogent, measurable goals and the development and empowerment of effective moral leaders to accomplish these goals.

In October of 2003, Chairman Adam Putnam of the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, held a hearing where he clearly identified the problem, saying, "The nation's health, wealth, and security rely on these systems, but, until recently, computer security for these systems has not been a major focus. As a result, these systems on which we rely so heavily are undeniably vulnerable to cyber attack or terrorism." Those vulnerabilities still exist today, only now they are less excusable. More importantly, the government's plan to secure our critical infrastructures from a cyber threat remains vague and formative despite clear legislative and executive mandates.

Since September 11, 2001, the focus of security in the United States has been on physical terrorist attacks. In contrast, the government's cyber security efforts have focused on the internet and networking and desktop functions we all use every day. Unfortunately, operational control systems, which are at the heart of our critical infrastructures, do not work like conventional desktop business computer systems. The President has spoken

to this in Homeland Security Presidential Directive #7 (HSPD-7) and the National Strategy to Secure Cyberspace, emphasize that our nation's critical infrastructures provide services which are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

Congress has also spoken through The Homeland Security Act of 2002 which laid clear mandate on Cybersecurity at Department of Homeland Security. The Act requires DHS to 1) assess our vulnerability to cyber attack 2) develop a plan to fix it and 3) implement that plan using measurable goals and milestones. In order to implement the plan the Department has the admittedly difficult task of engaging and securing action from diverse players, state and local governments, other federal agencies, especially key industry actors. Cyber vulnerability is primarily in the private sector and the Department must find a way to overcome the challenges there. The nature of terrorists is to attack private citizens as we recently saw in the horrific attack in the United Kingdom. There can be no excuse for not effectively engaging the private sector, even though it is hard. We ask no less of our food safety, airline security and pharmaceutical industries.

Nobody wants to micromanage the private sector; however, America expects DHS to take every reasonable measure to protect us from terrorism. I am not convinced that threshold has been met.

If America is to be safe from the damage of a cyber attack, we will need a plan, a budget tied to that plan and Congressional commitment to the

implementation of the plan. In particular, I hope we can commit to the following:

1. The completion of the National Infrastructure Protection Plan, fully incorporating the cyber component with more than vague generalities;

2. A way to measure milestones in the NIPP that will be assigned to a named department heads;

3. A budget line item associated with the milestones.

To that end, I look forward to hearing from our witnesses from GAO, DHS, the State of Delaware, and Siemens Power Transmission & Distribution, Inc.