

STATEMENT**Opening Statement of Ranking Member Fred Thompson****Hearing, "Critical Infrastructure Protection: Who's In Charge?"****Thursday, October 4, 2001**

I am pleased the Committee is holding these hearings. The topic – critical infrastructure protection – is particularly timely. We continue to see threats to our critical infrastructure becoming increasingly diffuse. And we are rightly focused on ensuring that greater safeguards are in place to protect us from attacks like those we experienced on September 11th.

We are looking at things through different glasses today. It is clear that it no longer takes a nation state to pose a real threat. Along with biological, chemical, nuclear, and conventional threats, we must place particular emphasis on cyberthreats now more than ever.

The President has shown tremendous leadership by establishing an organizational framework and assigning essential tasks. Whether it be a missile attack by a rogue nation or by terrorists, a suitcase bomb, a biological attack, or a cyber-attack, we must ensure that our citizens are protected. Cyber-security, although just one element of our complex, interconnected infrastructure, is critical. And, it is left to us to ask tough questions of those who we know are trying to do the right thing to protect our citizens from cyber-attack.

Too often it seems we focus on rearranging the boxes and creating new laws and new agencies. The appointment of Governor Ridge is a good step in the right direction. But we have a real organizational problem here in the federal government. The new Office of Homeland Security, and within it the Office of Cyberterrorism, will require appropriate authority, real leadership, and true accountability. We must also ask how the agency will work with the private sector.

Government basically cannot seem to manage large projects very well. We're told time and time again by GAO and the Inspectors General of the huge financial management problems we have, with billions and billions of dollars lost repeatedly to waste, fraud and abuse in the federal government. And we cannot manage large information systems either, with billions and billions more going down the drain year after year. Mismanagement is a government wide problem. We cannot expect to simply set up new systems and agencies perfectly, while the same existing agencies continue to appear on GAO's High Risk List. Unless we have leadership from the top with the right person in charge with meaningful authority and accountability, mismanagement will infect all new projects as well.

Government is great at setting goals, but terrible at implementing them. Today, I hope we explore plans being instituted to protect our critical infrastructure. If we plan properly and manage implementation of this process well, we can give the American people enough assurance that they and their critical infrastructure are safe. Hopefully we can learn from past experience and not continue to make the same mistakes again and again. I look forward

to hearing ideas on who should be held responsible for coordinating and managing these systems and how we can make this work.

[Committee Members](#) | [Subcommittees](#) | [Hearings](#) | [Key Legislation](#) | [Jurisdiction](#)
[Press Statements](#) | [Current Issues](#) | [Video of Select Hearings](#) | [Sites of Interest](#)