EDOLPHUS TOWNS, NEW YORK
CHAIRMAN

DARRELL E. ISSA, CALIFORNIA
RANKING MINORITY MEMBER

ONE HUNDRED ELEVENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

Majority (202) 225–5051
Minority (202) 225–5074

Opening Statement

Brian P. Bilbray
Ranking Member
Government Management, Organization, and Procurement Subcommittee

Hearing on
"Cybersecurity:
Emerging Threats, Vulnerabilities, and Challenges in Securing Federal Information Systems"

May 5, 2009

Thank you, Madam Chair.

This is a vitally important topic, and I appreciate the fact you have convened this hearing.

Vulnerabilities in critical infrastructures leave the United States open to significant economic disruptions. A cyber attack on the electric grid or computers used by the financial markets could be catastrophic. Even today, the nation loses an incalculable amount of money at the hands of cyber criminals.

There are also profound national security implications.

Recently, many press reports and evaluations by outside organizations have provided a grim prognosis of the state of the federal government's cyber weaknesses. We are told our computer systems are constantly being probed by adversaries. These intruders apparently seek to obtain data or to learn how to damage or manipulate key systems. There is evidence that some of these efforts have been successful. News accounts suggest that important military data and other information have been lost.

Today, we will hear more about these events.

It is essential that we ensure that this nation's computing and information systems operate properly and without interference from criminals or enemies. In our technologically advanced society, cyber systems are vital to the smooth functioning of our government, our businesses, and our private activities.

Our enemies surely know this.

For this reason, we must take steps to prevent cyber attacks. Failing to clearly and energetically prepare for this possibility leaves this nation vulnerable to damage even greater than that incurred on September 11, 2001.

Indeed, we must apply the lessons from that tragic day.

We have learned that government agencies with the responsibility of detecting and deterring terrorist attacks communicated poorly. In some instances, poorly conceived and executed policies had been enacted intentionally to inhibit the sharing of important information.

Such barriers, if they exist today in the government cyber realm, must be eliminated.

Maintaining the security of the information infrastructure is important across the country. However, I am especially proud of the important work being done in my Congressional district by leading corporations which have set the global standard for information security practices and products. I look forward to the possibility of future hearings on this topic in which we can learn from these companies and gain from their expertise.

I also am eager to hear from today's witnesses. These representatives from in and outside of government will help us assess federal cybersecurity and determine how it can be strengthened. I am particularly interested to hear the testimony of our private experts. I know they will tell us about business innovations and practices which can be applied to the government.

Madam Chair, thank you again for convening this hearing.