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
"The State of Federal Information Security"

May 19, 2009

Thank you, Madam Chair.

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

Every day, the United States is under attack. Hackers, terrorists, hostile foreign governments, and identity thieves raid our homes, bank accounts, and energy grids.

The evolution of cyberspace, a boon of innovation and prosperity, exposed a host of new vulnerabilities that now pose a serious threat to the economic and national security of the United States. This adaptive and faceless threat cannot be ignored and should be met with an efficient, flexible, and coordinated policy.

When it comes to information security, the federal government can and should be the leader. Enacted into law on December 17, 2002, as title III of the E-Government Act of 2002, FISMA requires each agency to create a comprehensive risk-based approach to agency-wide information security management. It is intended to make security management an integral part of an agency's operations and to ensure we are actively using best practices to secure our systems.

In recent years, we have started to see positive results.

In a recently released survey by the International Information Systems Certification Consortium, ninety percent of Chief Information Security Officers (CISO) felt they had a positive impact on their agencies' cybersecurity and many generally viewed FISMA positively.

But, to steal a favorite phrase from of our friends over at GAO, "inefficiencies remain."

Many of the CISOs surveyed found the compliance reporting under FISMA to be ineffective and urged a shift to continuous, real-time monitoring of IT systems. Similarly, the effort required to produce reports has proven both cumbersome and inefficient- diverting their valuable time and concentration to paperwork.

In recent weeks, witnesses from both government and industry have suggested that the United States must develop a more comprehensive national strategy to secure our critical information infrastructure and become a world leader in cyberspace. For many, part of this broad strategy is the modernization of FISMA.

If the testimony we have heard in recent weeks is at all indicative of the truth, the time for action is now. It would be a tragedy of quantifiable measure if one day we find ourselves asking the same questions we did on September 12, 2001- how did we not prevent this?

In reviewing some of the written testimony the witnesses have submitted for this hearing there is clearly reason to be concerned. When twenty-three of the 24 major federal agencies report weaknesses in their agency-wide information security programs steps must be taken to address these failings. I will look forward to hearing the recommendations of these witnesses.

The answers are out there. It is time for the United States to get information security right. I look forward to reviewing the Administration's 60-day review and engaging all branches of the federal government and private industry in a coordinated effort to develop a flexible, efficient, and sound policy to secure our information systems and critical infrastructure.

Madam Chair, thank you again for convening this hearing.