STATEMENT OF SENATOR JOHN MCCAIN, RANKING MEMBER

SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Hearing on "More Security, Less Waste: What Makes Sense for Our Federal Cyber Defense"

October 29, 2009

Senator Carper, thank you for holding this hearing today. As the sixth annual Cybersecurity Awareness Month comes to a close, it is an appropriate time for this subcommittee to examine how we measure the effectiveness of cybersecurity policies and procedures at our federal agencies.

The federal government relies heavily on complicated information systems for day-to-day operations. The risks posed to those systems have never been higher. Cybercrime and cyber espionage are on the rise. Indeed, nation-states seek to exploit our government networks, to steal sensitive intelligence or intellectual property for military and industrial advantage. A report prepared just this month for the bi-partisan US Chinese Economic and Security Review Commission concludes that the Chinese have made it a military priority to target the US Government and industry as part of a "long term, sophisticated, computer network exploitation campaign."

Recognizing these threats, the federal government is spending billions of dollars on information technology security each year. OMB estimates $6.2 billion was spent in fiscal year 2008 alone, nearly 10% of the entire cost of the federal IT investment portfolio.

Agencies spend a large percentage of their security budget and manpower on collecting data on compliance. Compliance with security standards and training mandates are necessary and can be useful for providing accountability and oversight.

Many experts, however, argue that these polices simply require that agencies have a security plan but do not measure that plan's effectiveness. This process has been described as a multi-million dollar paperwork exercise that certifies only that appropriate security measures are in place at a fixed point in time. In other words, a closet full of reports about the security of IT systems yesterday does not necessarily tell us how secure those same systems are today.

As we keep reading in media reports, the sophistication, frequency, and speed at which new cyber threats emerge have increased exponentially in just the last five years. To combat emerging cyber threats requires a continuous reevaluation of security priorities based on current risk. Agencies should not spend finite resources on reports that are outdated as soon as they are published. Most experts agree that only the continuous monitoring of security controls will both ensure compliance with federal policy and also achieve the accountability and real-time situational awareness that is critical for protecting our government networks.

I look forward to an informative discussion with our witnesses on new approaches that may accomplish that goal cost effectively.

Thank you Mr. Chairman.