Opening Statement by Harry D. Raduege, Jr., Lt. General, USAF (Ret)
Chairman of Deloitte Center for Network Innovation

Subcommittee on Government Management, Organization and Procurement
"Cybersecurity: Emerging Threats, Vulnerabilities, and Challenges in Securing Federal Information Systems"
Tuesday, May 5, 2009

Chairwoman Watson, Ranking Member Bilbray, and Members of the Subcommittee, thank you for the opportunity to join in today's hearing to discuss efforts to protect our nation from current and emerging cyber threats and vulnerability of our nation's critical infrastructures to exploitation, attack, and disruption. Relentless and continuing cyber intrusions into Federal government systems, defense industrial base companies, and supporting critical infrastructures continue to pose serious national security risks to our nation. And while I understand the main focus of this hearing is centered primarily on Federal government systems, I would also point out that cyber crime is an escalating problem that affects all citizens and businesses. The cyber threat has no boundaries. In fact, a variety of studies have identified the serious implications of cyber crime focused on stealing financial and personal information and the tremendous economic impact of this profit-driven activity. The problem of cyber threats affects not only our national security but also our economy and the privacy of all our citizens.

Cybersecurity is an issue that is front and center from a public policy perspective as the new Administration grapples with how to handle an overall national cyber strategy. Various reports have come out over the past several months, including the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. I was privileged to co-chair this Commission. This important effort provided findings and recommendations to secure cyberspace for the country and to help guide policy-making. It called for immediate action to create a comprehensive national security strategy for cyberspace. The new Administration has cybersecurity high on its agenda and is making a serious effort to take what has already been done and improve our national cyber posture. While I am hopeful, there is still much to be done. Improving the security of our Federal networks and nation's digital infrastructures will be a long-term effort, but immediate focused attention on this significant challenge is absolutely critical. As our Commission report noted, cybersecurity is now a major national security problem for the United States. In response, we need to focus all tools of national power – diplomatic, economic, military, intelligence gathering, and law enforcement -- on this critical issue.

I would like to briefly highlight three challenges facing the Federal government's information systems and critical cyber infrastructure assets.

First, despite the increased attention by this Administration and the 60-day cybersecurity review led by Ms. Melissa Hathaway, it is imperative that the Federal government be organized properly for the emerging threats and vulnerabilities in securing Federal information systems. Currently, our networks and systems are under continuous and relentless cyber assault. We are losing a significant amount of personal and sensitive data every day. Even worse, we are losing competitive advantage globally. The Federal government must become a model for cybersecurity, and it must start by securing our networks and information as quickly as possible. While efforts like the Comprehensive National Cybersecurity Initiative will bear fruit over time, we need leadership throughout the Federal government to make this a focus area. Securing our networks and protecting information on those networks is an important matter of public trust; and government must be well organized to lead.

Second, raising the level of education and awareness of the seriousness of the threats is imperative. Those who work in the cybersecurity business clearly understand the magnitude of the problems and are very concerned about the current state of affairs. However, for many in both government and industry, the threats are abstract, the implications are not fully understood, and their ability to help is unclear. An aggressive outreach and awareness campaign is needed in creating a cybersecurity mindset to raise the level of knowledge of Federal leaders and the workforce that our nation is constantly under cyber attack. We need to ensure that every person who logs onto a system connected to the Federal enterprise is properly educated and trained to protect the information in which they have been entrusted.

Third, there is a need for clearly delineated roles and responsibilities within the Federal government for cybersecurity. While the Administration is focused on addressing this concern, it is critical to ensure a successful cybersecurity strategy. A properly structured and resourced organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, military, intelligence community, and our nation's international allies to address incidents against critical cyber infrastructure, systems, and functions, is essential.

In summary, our nation and, in particular, Federal networks and systems are under relentless cyber assault. While many good efforts are underway, much more is needed, and faster. The Federal government must focus on understanding cyber risk and take appropriate action to secure its networks and become a model for others. Today, that is not the case. We also must change the culture of the Federal workforce by raising and maintaining the awareness of cyber threats that are focused on gaining access to our networks every day, 24 hours a day. And finally, we must clearly identify "who's in charge" with respect to Federal cybersecurity.

Madame Chair, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.