Opening Statement – Cyber Security Hearing

November 17, 2009

Thank you, Mr. Chairman, for holding this hearing on the important issue of cyber security. The federal government increasingly relies on interconnected information systems for crucial day-to-day operations, and these systems are ever more subject to cyber espionage and cybercrime.

China, in particular, is a growing threat to U.S. cyber security. A report published last month by the U.S.-China Economic and Security Review Commission stated, "Increasingly, Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict...China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. Government...”

This report goes on to say, “In a conflict with the U.S., China will likely use its computer network operations capabilities to attack...unclassified DoD and civilian contractor logistics networks in the continental U.S. and allied countries in the Asia-Pacific region. The stated goal in targeting these systems is to delay U.S. deployments and impact combat effectiveness of troops already in theater.”

The Chinese military could not beat our forces head-on, so it is clearly seeking another method to gain the advantage. The U.S. is not adequately countering this serious and growing threat.

During a recent interview on the news program “60 minutes,” the Director of the Technology and Public Policy Program at the Center for Strategic and International Studies said that the U.S. faced a so-called “electronic Pearl Harbor” in 2007 wherein an unknown foreign power broke into the computer systems at the Departments of Defense, State, Commerce, and Energy, and probably NASA, and downloaded the equivalent of a Library of Congress-worth of government information.

During the same news segment, when asked about the possibility that penetrations into U.S. systems had left behind malicious software that could enable future attacks, former Director of National Intelligence Mike McConnell responded, “I would be shocked if we were in a situation where the tools and capabilities and techniques had not been left in U.S. computer and information systems."

As with the threat from terrorism, our government must use all tools available to address this threat, and protect our citizens and way of life. A key challenge in this regard is balancing the privacy of U.S. citizens.

Representatives of the departments that are in charge of addressing cyber security vulnerabilities are assembled before the subcommittee today, and I look forward to hearing how they are planning to get ahead of the growing cyber threat.

Thank you, Mr. Chairman.