

**FOR IMMEDIATE RELEASE****Statement of Chairman Bennie G. Thompson*****Cybersecurity: DHS' Role, Federal Efforts and National Policy***

June 16, 2010 (Washington) – Today, Committee on Homeland Security Chairman Bennie G. Thompson (D-MS) delivered the following prepared remarks for the full Committee hearing entitled “Cybersecurity: DHS’ Role, Federal Efforts and National Policy”;

“Today’s hearing, entitled “Cybersecurity: DHS’ Role, Federal Efforts, and National Policy” will examine the Department of Homeland Security’s efforts to secure cyberspace. Since 1997, GAO has designated information security as a high-risk area in the federal government. Ten years later, information security is still high risk.

Some would say that it is the difficulty of this task that keeps us from achieving it. But I know that few things worth doing are easy. Securing the federal government’s networks from a wide array of cyber attackers is not easy. But few tasks are more necessary.

According to GAO, the cybersecurity incidents reported by Federal agencies have increased 400% in the last four years. From 5,503 incidents in FY2006 to about 30,000 incidents in FY2009. Whether the military or intelligence-gathering operations of foreign nations; domestic or international terrorist groups; lone wolf hate-driven individuals; common criminals, or thrill-seeking hackers, those attempting to infiltrate and exploit this country’s computer networks are both numerous and determined.

But they will not win if we match their determination with our resolve and defeat their abundance with our expertise. As the lead agency for cybersecurity in federal civilian agencies, the Department of Homeland security is responsible for guiding and directing the federal efforts to defeat this multi-faceted cyber enemy. So my question today is does the Department have what it needs to win this war?

US CERT—the office within the Department that is charged with leading our cyber defense efforts has significant deficiencies. It does not have sufficient staff to analyze security information. It cannot develop internal capacity because contractors outnumber federal employees by about 3 to 1. It has not developed leadership consistency because US CERT has had four directors in five years. Given these administrative failings, it should come as no surprise that day-to-day operations may suffer.

According to the President’s National Security Strategy released last month, Federal cyber networks must be “secure, trustworthy, and resilient.”

DHS must be a major actor in this nation’s efforts to secure the Federal computer networks. In addition to the Federal government, DHS must reach out to state, local and tribal governments as well as the private sector to assure the protection and resiliency our cyber infrastructure. But none of this can occur without adequate staffing, planning and funding. Today, we must pledge to become as committed to secure our networks as our enemies are committed to breach them.”

#

FOR MORE INFORMATION: Please contact Dena Graziano or Adam Comis at (202) 225-9978