

The Honorable Orrin G. Hatch
U.S. Senate Judiciary Committee -
Subcommittee on Crime & Terrorism:
Cyber Security: Responding to the Threat of Cyber Crime & Terrorism
April 12, 2011

Question To Entire Panel II:

As you know, there are multiple Senate Committees that are exploring how best to proceed on cyber security policy. I've been following this issue very closely and would appreciate learning your views on some the legislative proposal that are pending? What are some of the issues we should avoid and others we should embrace?

Phyllis Schneck Response:

Issue Summary: The cyber security threat landscape has changed fundamentally over the last decade. According to the Center for Strategic and International Studies, crime syndicates, terrorists, and nation states are engaging in cyber attacks to steal billions of dollars in intellectual property, disrupt businesses, and threaten governments. These sophisticated actors are capable of damaging or shutting down vital parts of the global economy. And the threat to national governments and critical infrastructures has never been greater. In response, policy makers are now engaged in a once in a decade revision of the nation's cyber security laws. They are considering a wide range of options that include updating rules governing the way Federal agencies manage cyber security, requiring critical infrastructure industries to upgrade their security regimes, creating a national, uniform system of breach notification, and increasing investments in university cyber security research and training.

McAfee Priorities:

Presidential Leadership: To date, no single individual or entity has been given the responsibility to coordinate all of the Federal government's cyber-security related activities. This has resulted in a patch-work of cyber security programs, some effective, and others less effective. We support the President's appointment of a Cyber Czar. For the Cyber Chief to be as successful as possible, he/she needs to be given direct access to the President and genuine authority or leverage over agency budgets. We likewise support legislation that would mandate the appointment of a Cyber Czar that reports to the President.

Agency Leadership: Holding the leadership of Cabinet Departments and independent agencies accountable for information security management is a vital objective. Each agency should have a Chief Information Security Officer (CISO) who has the authority and budget to continually upgrade security processes, technologies, and people to ensure that agency is sufficiently protected. Each agency CISO should be aligned with colleagues in the agencies and in the private sector to gain visibility into cyber events and trends, and have the capability to immediately take joint action in crisis situations. Each CISO should have a trusted public-private collaboration team assembled long before a crisis.

Agencies with cyber leadership responsibilities should be provided adequate funding to assemble "A players" in technology, and policy for rapid and effective execution. Leadership should be empowered to incentivize top talent and release resources that are not effective, removing political obstacles from needed progress, and making government work more attractive to the best minds in the nation.

FISMA: We have long supported the *Federal Information Security Management Act* (FISMA) process and believe that most agencies are doing their best to comply with the law. However, while FISMA compliance grades may have improved over the years, there appears to be a limited correlation between an agency's FISMA compliance and the state of its cyber security posture. We thus support Federal legislation to transform FISMA into an operational frame work that will help agencies produce continuous system and

process improvements that can be quantified and verified. Toward this end, agencies should be required to do an annual gap analysis that identifies deficiencies and provides program objectives and milestone plans to close these gaps. These reports should also address agency needs for additional resources and funding to ensure these gaps are closed. The executive branch should likewise continue to roll out its continuous monitoring model of information gathering that is effectively replacing paper reports as a means of delivering performance metrics.

Breach Notification: Forty-four states enforce breach notification laws. While these laws play a vital role in pushing organizations to improve their data management rules and processes, this system of state laws is inefficient and makes compliance difficult given their lack of uniformity. Congress should pass a uniform breach notification law. Such action would send a clear signal to the market on the need to improve data security practices, while also making compliance and enforcement predictable and efficient. Legislators should consider the merits of modeling their breach notification proposals on the rules that are already in place for medical information mandated by the Health Information Technology for Economic and Clinical Health Act or HITECH Act.

Standards: The global IT industry is fast moving and depends on rapid innovation to meet customer requirements. The government should defer to de-facto standards or to private sector standards setting bodies to ensure that IT companies can continue to develop products that meet the needs of global customers. Industry activities to rationalize assurance standards should also be supported by the government.

Any standards developed by the US government should be done in consultation with the private sector and should specify process, performance criteria or functional specifications, not specific products or technologies without duplication. NIST should collaborate with other government agencies that have unique expertise in cyber security (the Energy Department's expertise, for instance, in addressing electric and nuclear cyber-vulnerabilities) and take the lead in coordinating the Federal government's agenda in the development of international cyber security standards. Standards advocated by the US Government should be consistent with standards recognized by such international bodies as ISO.

Special attention should be paid to what has led to success in more narrowly defined arenas. For example, the Department of Defense and the National Security Agency have developed a seven-zone defense in depth security architecture with mandated functional protections in each area. At a minimum, US Federal Civilian agencies and Defense Industrial Base entities should be mandated to use the same standards. The Department of Homeland Security and DC3 should be charged with managing compliance audits and enforcement of these standards.

Public/Private Partnership on Information Sharing and Information Exchanges: To further promote public/private partnerships, existing government bodies should be leveraged in a more streamlined way. The Enduring Security Framework, a body to which McAfee belongs, is a success and should be used as best practice model. The public/private partnerships managed by the Department of Homeland Security should be streamlined and up-leveled to ensure that senior corporate officials and senior government officials are positioned to share vital information and best practices. Furthermore, too often the current legal system acts as a disincentive for productive information sharing. Liability reforms need to be enacted to help incent companies to share vital information on cyber security threats with their government counterparts.

Department of Homeland Security Einstein 3: Commercial off the shelf technologies (COTs) have proven their ability to protect the most sensitive government sites and IT systems. For instance, COTs is the basis of Department of Defense's Host Based Security System, one of the most successful cyber security implementations in the Federal government. Einstein 1 and 2 have been based on a proprietary technology sponsored by the government, and these programs have consistently failed to meet expectations. Einstein 3 should include COTs solutions, and they should be mixed and matched with government proprietary technologies as appropriate to enable the Department of Homeland Security to roll out a world-class cyber security program.