



January 2010

## Cybersecurity Will Continue to be Hot Topic in 2010

## CYBERSECURITY ALERT

**Executive Summary**

Cybersecurity issues continue to be on the forefront of the minds of the Obama Administration and the Congress. These issues affect everyone in the country, from states, counties and municipalities to non-profit institutions like hospitals to the private sector (which owns 85 percent of the nation's infrastructure). Each segment relies on their systems to protect those they serve across the nation's infrastructure. As a result, millions of hours of human capital and billions of dollars within the Executive Branch are being spent to find better, smarter ways to address this issue.

What does this mean for you? It means that it is critical to engage with the government and to offer the government real-time information that can help the decision-making process as they go forward. It also means everyone could be subject to potential additional regulations and security mandates that should make every company stand up and actively participate in this process.

**The end of 2009 was dominated by a series of actions on the part of the Executive Branch and the Congress.****U.S. Congress**

Congress continued to express their concerns over the need for a comprehensive cybersecurity framework. Senate Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman (I-CT) and Ranking Member Susan Collins (R-ME) announced their plans for a comprehensive cybersecurity bill.

Sen. Lieberman previewed a measure he plans to introduce in 2010 before the U.S. Chamber of Commerce Cybersecurity Task Force. Lieberman outlined the five principles of his proposed cybersecurity bill. They include: 1) a Senate-confirmed cybersecurity coordinator in the Executive Office of the President; 2) authority and personnel for DHS to monitor federal civilian networks and defend against malicious traffic; 3) a mandatory risk-based approach, established by DHS, to ensure the nation's critical infrastructure, including financial systems, electric power and mass transit, and voluntary guidance for less critical companies; 4) new acquisition policies to tighten the security of government systems, including procurement reform that requires vendors to comply with security standards when selling technology solutions to federal agencies; and 5) a recruitment strategy for hiring, retaining and training cyber security personnel in the federal government.

The Congressional agenda is full of varying proposed cybersecurity legislation and it is unclear with a full homeland security agenda, and the recent aborted terrorist attack on Christmas Day, how quickly these bills will be able to move through committee and be signed into law. However, suffice it to say that cybersecurity will continue to be at the forefront for the White House, Executive Branch and Congress for some time.

**Executive Branch Activities**

October of 2009 was dubbed "National Cybersecurity Awareness Month", which also highlights the U.S. Department of Homeland Security (DHS) unveiling the long-awaited CyberCenter. The \$9 million operations center based in Northern Virginia will help to better coordinate the government's response to cyber attacks. It also merges the U.S. Computer Emergency Readiness Team (CERT) and the National Coordinating Center for Telecommunications to monitor government networks to work better together. U.S. officials have said that government computer systems are probed or

*This Cybersecurity Alert provides only general information and should not be relied upon as legal advice.*

*For more information, contact your Patton Boggs LLP attorney or the author listed below.*

Norma M. Krayem  
202-457-5206  
[nkrayem@pattonboggs.com](mailto:nkrayem@pattonboggs.com)

[WWW.PATTONBOGGS.COM](http://WWW.PATTONBOGGS.COM)

scanned millions of times a day, and face an increasing threat from hackers, cybercriminals looking to steal money or information and nation-states aimed at espionage or the destruction of networks that run vital services. The goal is a more coordinated effort by the federal government to monitor and protect U.S. systems and work with the private sector to ensure that transportation systems, energy plants and other sensitive networks are equally protected. Over time, the Center will also include the National Cybersecurity Center, which coordinates operations among the six largest federal cybercenters, the DHS Office of Intelligence and Analysis and representatives from the private sector.

The Office of Management and Budget (OMB) and the White House announced plans to introduce new tools and metrics for measuring and managing the federal government's cybersecurity efforts. Earlier in 2009, OMB released "CyberScope" a tool that allows federal agencies to report Federal Information Security Management Act (FISMA) compliance via an authenticated Web-based reporting tool rather than sending spreadsheets via e-mail. Agencies are required to report detailed spending information on cybersecurity this fiscal year. Next spring, that information will make its way to a federal cybersecurity "dashboard" similar to the IT Dashboard, a public Web site launched earlier this year to track federal IT spending and project performance. There has been criticism that the government's implementation of FISMA focuses too much on paperwork and on having certain tools and processes in place, and not enough on performance. Early in 2010, performance metrics will be established to ensure more focused measurement on progress and government-wide achievements.

The Homeland Security Act of 2002, Homeland Security Presidential Directive (HSPD-7) and the National Strategy to Secure Cyberspace gives DHS the lead on efforts to protect cybersecurity for critical infrastructure. The Government Accountability Office (GAO) has analyzed the DHS' cyber security efforts and identified a series of areas they believe the agency needs to address. Since that time, the agency continues to move ahead to solidify its oversight of cybersecurity, with DHS Secretary Janet Napolitano announcing that the agency has been cleared to hire at least 1,000 new cybersecurity professionals over the next three years to fill staffing gaps at various DHS agencies. Her focus is to drill into key risk areas such as "cyber risk and strategic analysis, cyber incident response, vulnerability detection and assessment, intelligence and investigation, and network and systems engineering."

GAO also focused on the role of the U.S. Department of Commerce's National Institutes of Standard's (NIST) responsibilities under FISMA, and identified a series of key information security standards and guidelines that the agency has moved forward on in the last few years.

The recent announcement by the White House of the New "Cyber Czar" Howard Schmidt is an important step forward and there will be many challenges going forward to manage this issue government-wide. The Congress had previously expressed some concern over the growing number of "czars" at the White House, and has argued that they should all be subject to Senate confirmation.

---

This Cybersecurity Alert provides only general information and should not be relied upon as legal advice. For more information, contact your Patton Boggs LLP attorney or the author listed below.

**Norma M. Krayem**  
202-457-5206  
[nkrayem@pattonboggs.com](mailto:nkrayem@pattonboggs.com)

WASHINGTON DC | NORTHERN VIRGINIA | NEW JERSEY | NEW YORK | DALLAS | DENVER | ANCHORAGE | DOHA, QATAR |  
ABU DHABI, U.A.E.