

Just Released!

BlackBerry Enterprise Server v5.0

Get it Today

Upgrade Now

Or Try a Free Trial

Download Now

 BlackBerry.

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Cybersecurity Review Finds U.S. Networks 'Not Secure'

The report dovetails with President Obama's call for the creation of a cybersecurity coordinator who will orchestrate and integrate federal cybersecurity policies and agendas.

By Thomas Claburn, [InformationWeek](#)

May 29, 2009

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=217700860>

The White House has released [a report](#) calling for urgent action to secure the nation's [computer](#) network infrastructure.

The report covers the findings of a 60-day review of national cybersecurity policy and practice by Melissa Hathaway, a member of the National Security Council (NSC) and the acting White House cybersecurity chief. The report dovetailed with President Obama's [announcement](#) Friday of the creation of a cybersecurity coordinator who will orchestrate and integrate federal cybersecurity policies and agendas.

"The [architecture](#) of the nation's digital infrastructure, based largely upon the Internet, is not secure or resilient," the report says. "Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations."

The report characterizes cyberthreats as one of the most serious economic and national security challenges of the 21st century. Military leaders have made similar warnings to Congress in recent months.

Shortly after Obama appointed Hathaway, the government's cybersecurity director, Rod Beckstrom, resigned. The former Silicon Valley entrepreneur was appointed in March 2008 to run the National Cyber Security Center (NCSC), a group created to oversee national cybersecurity. In his [resignation letter](#), Beckstrom criticized the lack of funding for the NCSC and the National Security Agency's dominant role in cybersecurity initiatives. "[T]he threats to our democratic processes are significant if all top-level government [network security](#) and monitoring are handled by one organization," he said.

Lawmakers and cybersecurity experts have spoken out about cybersecurity problems for years, but the government's piecemeal responses to date haven't kept pace with cybersecurity threats. Recent reports about the [vulnerability](#) of the air traffic control system and the electrical grid, not to mention frequent breaches of government and private-sector systems, have led to repeated calls for strong leadership from the White House.

For example, a cybersecurity report released in December by the Center for Strategic & International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency, warned that America is losing the battle to protect cyberspace. It said that cybersecurity "is a strategic issue on par with weapons of mass destruction and global jihad" and that it "can no longer be relegated to [information technology](#) offices and chief information officers." Hathaway's report addresses that concern, calling for White House leadership rather than delegating the task to the military or an intelligence agency. It also emphasizes the need to consider [privacy](#) and civil liberties interests as [cyberspace](#) policies are formulated and enacted.

The report calls for:

- The appointment of a cybersecurity policy official with dual roles in the NSC and the National Economic Council who will oversee national cybersecurity policies and initiatives.
- The development of an updated national strategy to defend cyber-infrastructure.
- Making cybersecurity a presidential priority and establish performance metrics.
- Appointing an official in charge of privacy and civil liberties issues to the NSC cybersecurity directorate.
- Ensure that policies and legal rules are in place to allow cybersecurity issues to be dealt with across government agencies.
- Launch a cybersecurity public-awareness and education campaign.
- Develop government positions and international relationships to promote international cybersecurity.
- Develop a cybersecurity incident response plan.
- Develop a White House-led process to promote new cybersecurity technologies.
- Work toward an [identity management](#) system in cyberspace that addresses privacy and civil liberties interests.

Patricia Titus, chief [information security](#) officer at [Unisys](#), the first CISO at the NSA, and a contributor to the CSIS report last year, said she was very encouraged by the report. Through Hathaway's report contains no real surprises, she said, the call for presidential attention to cybersecurity is essential. "If you can't get attention from your executives, you can't be success," she said.

Other security industry executives, like Symantec president and CEO Enrique Salem, echoed that sentiment.

Though Obama was critical of the Bush administration's cybersecurity efforts during his campaign last year, Titus credits the previous administration with laying a foundation, through initiatives like the Federal Information Security Management Act, that will support the current administration's efforts. She lauded the report for building on previous cybersecurity efforts. "When it comes to IT security, you can't stop and start over again," she said. "It's got to be continuous."

Acknowledging that there's contention about whether cybersecurity risks are exaggerated, she said that better information sharing is necessary to help officials and the public make informed decisions about cybersecurity policy. "Information needs to flow more freely," she said, echoing recent government reports on information sharing. "There's not much we can do in the industry about threats if we don't know what they are."

She agreed with the report's recommendation to better educate the public about cybersecurity issues.

A consequence of education, however, may be responsibility, particularly for businesses. The report suggests that a possible incentive to improve the situation might be "increased liability for the consequences of poor security."

Black Hat is like no other security conference. It happens in Las Vegas, July 25-30. [Find out more and register.](#)



The day of electronic health records is here.
We've been training for this mission 20 years.