

## COMPUTERWORLD

### **DHS exec's resignation raises red flags on NSA's cybersecurity role Critics contend that the spy agency shouldn't take the lead on federal cybersecurity efforts.**

By Jaikumar Vijayan

March 16, 2009 (Computerworld) The abrupt resignation of one of the U.S. government's top cybersecurity officials has exposed widespread -- though not universal -- opposition to the National Security Agency's expanding role in federal security initiatives.

Rod Beckström stepped down as head of the National Cybersecurity Center on Friday, six days after his one-year anniversary in that job. The Department of Homeland Security made him the NCSC's first director after setting up the agency to oversee the government's cybersecurity defenses and cyberthreat responses. But in a sharply worded resignation letter dated March 5, Beckström said the NSA is effectively running those efforts.

He also claimed that by proposing that the offices of both the NCSC and the National Protection and Programs Directorate be moved to its headquarters, the NSA is trying to wrest further control from the DHS.

Letting the intelligence agency take the lead on cybersecurity is "a bad strategy on multiple grounds," Beckström contended. The intelligence culture is "very different than a network operations or security culture," he wrote, adding that the NSA should be involved in cybersecurity programs but not have control over them.

Similar sentiments were voiced at a congressional hearing on cybersecurity issues last week. For instance, Scott Charney, vice president of Microsoft Corp.'s Trustworthy Computing initiative, noted that the NSA has more technical expertise on cybersecurity than other agencies do. But to ensure that the security work is "being done in a transparent fashion, the mission cannot rest with the NSA," Charney said.

Historically, intercepting and analyzing foreign communications has been the NSA's primary responsibility. As a result, it focuses more on covert data collection than on the information-sharing needed to build effective security defenses across the government and in the private sector, other critics said in interviews.

The NSA's "strength lies in breaking into networks," said Gartner Inc. analyst John Pescatore. And while the agency's top-secret nature is obviously appropriate for spying, it's the "exact opposite" of what is required on cybersecurity initiatives outside of the military, he said.

The NSA does have an information assurance unit that coexists with its eavesdropping operations and provides a wide range of security technologies and services, including vulnerability analysis and a 24/7 threat warning capability.

But those dual roles may conflict with each other, claimed Bruce Schneier, chief technology officer at security services vendor BT Counterpane. Citing a hypothetical example, Schneier wondered what the NSA would do if it found a flaw in Windows that would let the agency monitor electronic communications. "Do they fix it or do they exploit it?" he asked.

In testimony last month before the House Permanent Select Committee on Intelligence, Dennis Blair, who became director of national intelligence in January, acknowledged that many Americans don't trust the NSA to protect data. But he said that it has "the greatest repository of cyber talent" in the government and that its capabilities should be "harnessed and built on."

The NSA also has its supporters outside of the government. For instance, Alan Paller, director of research at the SANS Institute, a security research and training organization that has worked jointly with the NSA, said the leadership shown by the agency and the Department of Defense has been "the only bright spot in a desolate federal cybersecurity landscape."

And it's not like the DHS has a lot of fans -- the agency was roundly slammed at last week's hearing. David Powner, director of IT management issues at the Government Accountability Office, said it's obvious that the DHS isn't living up to its leadership responsibilities on cybersecurity.

In a statement, the DHS voiced regret about Beckström's departure and defended its ongoing security efforts. The agency said that it "has a strong relationship with the NSA and continues to work in close collaboration with all of our federal partners on protecting federal civilian networks."

All eyes are now on a 60-day review of federal cybersecurity programs that President Barack Obama ordered last month. The president is seeking recommendations for ensuring that the programs are aligned with government and private-sector needs. Then he gets to decide how big of a role both the DHS and the NSA will play in the future.