

## Multiple cybersecurity reforms launched

By GREGG CARLSTROM

June 22, 2009

The Obama administration and Congress have launched several initiatives that will radically transform the government's approach to cybersecurity:

- The White House's soon-to-be-established cybersecurity office is planning changes to the government's cybersecurity policies, and President Barack Obama will soon name a cybersecurity official to coordinate federal policy.
- The National Security Council, for the first time, is developing a response plan for cyberattacks.
- The Defense Department will invest tens of millions of dollars in cybersecurity research over the next few years — and may soon launch a new operational command dedicated to fighting cyberwars.
- The agency responsible for setting cybersecurity standards for federal agencies — the National Institute of Standards and Technology — issued security controls June 12 to protect agencies' networks from cyberattack.
- And Congress is working to rewrite the Federal Information Security Management Act (FISMA), the primary law governing federal cybersecurity activities. The bill — FISMA 2.0, some are calling it — would give chief information officers more power and more control over their IT budgets.

Taken together, these initiatives will allow the government to be more aggressive and efficient in confronting cyberthreats. Critics have long argued such changes are needed to transform a cybersecurity regime that they call bureaucratic, sluggish and outdated.

The changes come at a crucial time. Cyberattacks are increasing: There were 37,000 cyberattacks in the U.S. in 2007, the most recent year for which national data are available. That was an 800 percent increase from 2005.

And countering these attacks, many of which target the government, is costly for federal agencies: The Defense Department alone will spend more than \$200 million this year protecting its networks.

The new FISMA legislation, the Information and Communications Enhancement Act, was introduced by Sen. Tom Carper, D-Del., in April.

Erik Hopkins, a staff member on the Senate Homeland Security and Governmental Affairs Committee, said the biggest change would be "greater accountability." Critics of FISMA have long accused it of giving CIOs too much paperwork and not enough real power to oversee their networks.

The proposed changes in the Carper bill would address those concerns by giving CIOs more budget control and streamlining the guidance and compliance requirements imposed on CIOs.

Hopkins said the legislation will require CIOs to continuously monitor their networks for security vulnerabilities. That will mean more upfront work — agencies have to develop and install monitoring systems — but it will make it easier to prove FISMA compliance in the long run.

CIOs would also have more control over agency technology budgets. For example, a CIO could cut funding for technology projects that are headed for failure.

“We’re trying to strengthen the office so they have the ability, if needed, to effect change within the organization,” Hopkins said. “And we’re recognizing that [CIOs] only have two things: budget, and the ability to shut the system down.”

The legislation would give CIOs the ability to shut down parts of their networks that become compromised. It would also allow them to take proactive steps, such as barring contractors from their networks if the contractors don’t meet federal cybersecurity guidelines.

“We end up with the user being the last line of defense against many of these attacks,” said Susan Alexander, chief technology officer in the Office of the Deputy Assistant Secretary of Defense for Information and Identity Assurance. “We need to be able to cordon off pieces of our networks from each other so that, if bad things happen, we can cordon off those bad things.”

NIST is also working with the Defense Department to standardize cybersecurity controls for the entire federal government. The controls are recommended security settings for hardware and software; agencies use them to configure their networks.

Right now there are three sets of controls: one for civilians, one for Defense, and a third for the intelligence community. Experts say that creates a headache for contractors, who need to design different versions of their software to comply with each set of controls.

NIST took a first step toward fixing that problem earlier this month. It released a new version of Special Publication 800-53 — its list of recommended cybersecurity controls — including controls for national security agencies.

“It’s really an incredible cultural breakthrough to say, we’re not going to have a separate process at Defense, we’re going to trust the other parts of government,” said Tony Sager, chief of the National Security Agency’s vulnerability analysis and operations group. “There’s always this belief that, well, my problem is different than your problem ... and we have to get over that.”

Ron Ross, the FISMA project leader at NIST, said the new controls will also help agencies close some major “attack vectors” — common vulnerabilities that hackers use to break into networks.

There’s also movement on cybersecurity in the White House — even before the “czar” is named. The National Security Council and Homeland Security Council are writing an incident response plan that will coordinate the government’s overall response to a cyberattack.

That was one of the recommendations from the recently released review of federal cybersecurity policy. Melissa Hathaway, the official who led the review, said the plan will fix the government’s uncoordinated response to attacks.

Hathaway frequently talks about the government’s clumsy response to Conficker, the worm that spread across millions of computers around the world.

The government had no coordinated plan for dealing with the worm before it activated April 1; some federal agencies did nothing to clean their systems or prepare for the activation, despite knowing about the worm for months.

“We’re working on our incident response plan ... and we’re going to have the private sector red-team it,” said Hathaway, the acting senior director for cyberspace in the National Security Council. Red teams are teams of experts who pose as hackers and attack government systems to probe for weaknesses.

The private sector will also be involved in writing the plan, according to Hathaway.

“There’s a number of things the government hasn’t thought about that should be part of those chapters,” she said. “I’m talking with [federal chief technology officer] Aneesh Chopra about setting up a wiki to help develop it with the private sector, so [they] can contribute to it.”

The Defense Department has been talking about a “cyber command” for a few months; the new command would coordinate cybersecurity efforts across all of the military services and Defense agencies. But, at press time, Defense Secretary Robert Gates still hadn’t decided whether to move forward with the idea.

Individual services have already announced their own cybersecurity programs: The Army created a cyber office at the Pentagon earlier this year, and the Air Force said it will likely create a new cybersecurity headquarters at Lackland Air Force Base, Texas. And the Navy has its own Cyber Defense Operations Command.

Deputy Defense Secretary William Lynn stressed that the new command, if created, would not have jurisdiction outside of the Defense Department.

Critics of the proposal — on Capitol Hill, in federal agencies and in the private sector — have expressed concern that the cyber command would trample civilian agencies and pose a threat to civil liberties.

“It would not be the militarization of cyberspace. ... It would in no way be the Defense Department trying to take over the government’s cybersecurity,” Lynn said in a June 15 speech at the Center for Strategic and International Studies. “The responsibility for protecting federal civilian networks would remain with [the Homeland Security Department].”

Defense officials are also working to incorporate cybersecurity into the upcoming congressionally mandated Quadrennial Defense Review, scheduled for release in 2010. Many of the military scenarios used in formulating the review are being updated to include cyberattacks, Lynn said. Some of the scenarios will also include red teams from the Pentagon.

“We’ve taken the conventional military scenarios and added a cyber component to those,” Lynn said. “We have a red team. ... They are doing a red team analysis of those same scenarios, and they have a heavier emphasis on cyber[security].”

Some of these scenarios will eventually play out on the National Cyber Range, an Internet simulator being developed by the Defense Advanced Research Projects Agency. DARPA awarded nearly \$30 million in contracts earlier this year to seven firms, including Lockheed Martin and Northrop Grumman, which are developing prototypes of the range.

“This will allow us to engage in real-world simulations and field new leap-ahead capabilities for cybersecurity,” Lynn said.