Information Security

Full strategic report at:

www FCW.com/InformationSecurity2010

Inside:

CNCI2 Fills in Cybersecurity Blueprint

When President Obama launched a review of federal efforts to mitigate the economic and national security challenges caused by cybersecurity issues he made it clear that this country must:

- Establish a shared situational awareness network that identifies vulnerabilities, threats and events.
- Enhance U.S. counterintelligence capabilities and increase security of the supply chain
- Expand cyber education

On the recommendations of the Cyberspace Policy Review the government has begun to build on the Comprehensive National Cybersecurity Initiative (CNCI) as part of CNCI2 and this spring the White House released details of what agencies and the public can expect.

Manage the federal enterprise network as a single network enterprise with Trusted Internet Connections. Led by OMB, the TIC initiative will consolidate the government's external access points to create a common security solution. Agencies can do this as TIC Access Providers, operating it themselves, or by using commercial Managed Trusted IP Service (MTIPS) providers found in GSA-managed NETWORX contract.

Deploy an intrusion detection system of sensors across the federal enterprise. As part of EINSTEIN 2, DHS is deploying signature-based sensors that can inspect Internet traffic coming into federal systems to unearth unauthorized access and malicious content.

Pursue deployment of intrusion prevention systems across the federal enterprise. Aimed at civilian departments and agencies of the federal Executive Branch, EINSTEIN 3 will inspect packets and make decisions on the threat of network traffic over executive branch networks.

Coordinate and redirect research and development (R&D) efforts. Coordinating cyber-related R&D activities across government agencies is no easy task. This initiative tackles identifying those activities and directing R&D where it's needed.

Connect current cyber ops centers to enhance situational awareness. Government information security offices and strategic operations must share information on malicious activities and accommodate privacy protections to determine the threat against government then exploit different agencies' unique abilities to provide cyber defense. Responsibility for securing government networks will fall under the umbrella of the National Cybersecurity Center (NCSC) in the Department of Homeland Security.

Develop and implement a government-wide cyber counterintelligence (CI) plan. Aimed to coordinate across federal agencies, the plan will "detect, deter, and mitigate the foreign-sponsored cyber intelligence threat to U.S. and private sector information systems" by expanding "cyber CI education and awareness programs and workforce development to integrate CI into all cyber operations and analysis, increase employee awareness of the cyber CI threat, and increase counterintelligence collaboration across the government."

Increase the security of classified networks. They store the government's most sensitive data so any breach could seriously compromise national security.

Expand cyber education. Technology is a must for a solid security strategy but it is people that execute it. The government needs more cybersecurity experts. Recommendations include a national strategy.

Define and develop enduring "leap-ahead" technology, strategies, and programs. The government will seek strategies and programs to enhance R&D for high risk/high payoff solutions to cybersecurity issues that are the most pressing. Under this initiative, new technology should be deployable within five to 10 years.

Define and develop enduring deterrence strategies and programs. This component encourages government to take a long-range approach to cybersecurity. Among the initiatives: improve warning systems, define the roles of both the private sector and international entities and determine responses.

Develop a multi-pronged approach for global supply chain risk management. Globalization has extended to information and communications technology so the U.S. must be able to manage risks that spring from domestic and globalized supply chains.

Define the federal role for extending cybersecurity into critical infrastructure domains. Privately owned and operated critical infrastructures are critical to carrying government's mission to serve its people. This Initiative extends and expands the "partnership between the federal Government and the public and private sector owners and operators of Critical Infrastructure and Key Resources (CIKR)." The Department of Homeland Security in concert with private-sector partners have a plan for shared action that includes "aggressive" milestones. ❑

Security is a Matter of Policy

If any government agency doubted the need for and importance of an airtight security policy, the recent porn scandal at the Securities Exchange Commission was a dramatic wake-up call.

Agencies are well aware of threats to their security and have made it a point of urgency. In a survey conducted by the 1105 Government Information Group last fall, the 109 respondents consistently ranked security among their top three main concerns and almost always placed it first on agency budget priority lists. Sometimes the biggest threats to security come from within and agencies must take steps to ensure that employees know the rules and play by them. Most survey respondents, 85 percent, said their agencies conduct regular IT security compliance training.

For all the talk surrounding information security, as the SEC debacle has shown, policy and enforcement have lagged far behind the growing threats from both rapidly changing workplaces and technology advances. In past surveys conducted by the 1105 Government Information Group, respondents consistently said they knew their agencies had a security policy but many were simply not familiar with it. That must change if agencies are to protect the information that passes through their doors.

Setting IT Straight

There are a few steps that an agency should take to build and enforce a security policy.

Review existing policy. There's no need to re-invent the wheel. Agencies should first assess existing policy and determine where the holes or vulnerabilities might be, then fill the gaps. A security policy should be solid but also flexible enough to accommodate changes in work environments and technology.

Socialize. Cruising porn on government computers is a clear violation of any agency's policies, security or otherwise. But what of Facebook, YouTube and other social networking media? They can help workers connect with citizens, disseminate information, become more responsive and help agencies meet President Obama's mandate for more a more nimble and transparent government. Today's government workers are armed with technology and unprecedented access to outside sources. Any security policy must include very specific guidelines for accessing and using social media at work.

Assign responsibility. By now, agencies understand that policies are more easily adopted if someone is in charge. In an 1105 Government Information Group survey last year, 87 percent of the respondents said their agencies had a Chief Information Security Officer. And a recent study by the Information Systems Security Certification Consortium Inc. found that the CISOs have gained authority and do believe they are having a positive impact on their agencies.

Train, train, train. Security threats change and so do policies, making it crucial that employees are trained regularly regarding security guidelines and agency expectations.

Enforce the rules. There should be clear consequences for security violations and an agency must follow through with the stated reprimands and penalties.

Ramp up Resources. A strong security policy needs the proper technology and human resources behind it. Security officers need the most current technology for monitoring and ensuring compliance. And training as well as enforcement requires staffing up. But budgets are tight. Judicious use of tech budget dollars and discrimination when purchased new products and services can keep costs down. Many agencies employ contract workers to help with training and enforcement. ❑

Readying FISMA for an Extreme Makeover

A pair of recent initiatives have trained their sights on Federal Information Security Management Act, promising to reform the much beleaguered set of security requirements to which agencies must comply. First, the Office of Budget and Management issued a new set of security guidelines that brought changes to the reporting requirements. Among other things, agencies will be required to continuously report online their cybersecurity efforts.

Now, the National Defense Authorization Act, which has an amendment to create an Office of Cyberspace in the White House tucked away in it, was approved by a healthy margin by the U.S. House of Representatives last month.

Rep. James Langevin, D.-R.I. and Rep. Diane Watson, D.-Calif., who sponsored the amendment that includes Office of Cyberspace initiative, have made it clear that it is time to overhaul eight-year-old FISMA and bring security under a more comprehensive umbrella.

"These provisions will establish strong, centralized oversight to protect our nation's critical information infrastructure and update our comprehensive policy for operating in cyberspace," Langevin said in a statement.

Government agencies have long made it clear that while adhering to FISMA requirements does seem to boost security, the compliance reporting required is cumbersome, time-consuming and costly. By some estimates filing costs about $1,400 per page. Under the new guidelines, instead of submitting paper-based compliance reports at regular intervals, agencies will report on their security efforts and submit updates every month through CyberScope, a Web-based portal that will be overseen by the Department of Homeland Security. Not only will the new automated process eliminate burdensome paperwork but it will allow an agency to present a nearly real-time view of its security status.

The changes will also empower CISOs, giving them greater latitude in gathering data from different departments and bureaus within their agencies.

Agencies applauded the new initiative, with NASA quickly announcing its plans to break from the traditional paper-based reporting structure.

In a memo, Jerry Davis, deputy chief information officer for IT security at NASA, said the move will give NASA and other agencies the opportunity to gain a "near real-time understanding of risk posture, and not the production of paperwork."

He also noted that the old certification and accreditation system was simply not working and indeed were "largely ineffective" and didn't "ensure a system's security."

The government contends that the proposed reporting changes will rectify that. And the amendment included in the National Defense Authorization Act currently making its way through Congress promises to add top-down support and accountability to FISMA, creating a National Office for Cybersecurity and a Federal Cybersecurity Practice Board that will guide agencies in meeting FISMA reporting requirements.

"Not only does this amendment make necessary and wholesale improvements to our current cybersecurity policy and management framework, but it will also ensure that agencies have a strong leader within the Executive Office of the President to assist them in their efforts," said Watson in a statement.

But the Act still has to pass the Senate and it is unclear how easily it will do so…or if it will. The initiative also includes an amendment to end the military's "Don't Ask, Don't Tell" policy, a potentially controversial directive sure to make some senators uncomfortable. That could potentially put the kibosh on the legislation. ❑

Bill Paves Way for NIST Restructuring

Proposed restructuring of the National Institute of Standards and Technology (NIST) promises to have a strong impact on the federal government's cybersecurity efforts.

The House of Representatives in the spring signed off on The America COMPETES Reauthorization Act proposes to restructure NIST, reducing its number of laboratories from 10 to six. The Information Technology Laboratory would remain virtually the same, continuing to develop standards and measurements that ensure interoperability and security among other things. The lab's structure will also serve as a blueprint for other NIST labs.

"This bill authorizes a lab structure of six operating units to promote efficiency and a cross-disciplinary culture at NIST," said Rep. David Wu, (D-Ore.), sponsor of the NIST portion of the bill. He noted that the current NIST structure "no longer reflects today's technology sectors or the inherent and increasing multi-disciplinary nature of technology."

The NIST provision in the Act intends to empower the standards body. If the legislation is approved by the Senate, NIST Director Patrick Gallagher will be elevated to under-secretary for standards and technology within the Department of Commerce, a move that Wu said would "help inject NIST expertise into the administration's discussions on innovation, standards and support for high-tech growth." In fact, Gallagher would be tapped to help develop and reach international technical standards objectives. The Act also makes it clear that business and industry are not required to employ NIST's cybersecurity guidelines.

The bill has taken a long route through Congress, rejected in two previous House votes as being too expensive and containing controversial measures. Efforts to reject the bill were criticized by lawmakers with Bart Gordon, chairman of the House Science and Technology Committee, noting that at least one motion was "about gutting funding for our science agencies."

Lawmakers reworked the legislation to allow their peers to vote on some measures separately and the bill was approved by a healthy margin. ❑

The CISO Rises to the Top

Practically a foreign concept a decade ago, the Chief Information Security Officer (CISO) has become a solid fixture within federal government and has gained clout as agencies have made information security a top priority.

Experts contend that a critical part of any agency security policy and strategy is to have someone in charge of implementing, monitoring and ensuring that policy is carried out. And agencies have taken that to heart. A survey by the 1105 Government Information Group last year found that 87 percent of the respondents had a CISO or CISO-equivalent in place.

But unfortunately, if the CISO position wasn't simply a figurehead, it was close. Most lacked the authority to even gather information critical to security and compliance from deep within in the ranks of their own agencies. But that has changed…significantly.

In a report published last year by (ISC)^2, "A View from the Front Line: The State of Cybersecurity from the federal Chief Information Security Officer's Perspective," 90 percent of the respondents said that they had significant influence on their agency's security strategy.

"The CISOs' responses clearly demonstrate that cybersecurity is evolving in terms of management priority," said W. Hord Tipton, executive director of (ISC)^2, an organization which educates and certifies security professionals. "Although CISOs are still facing organizational challenges, we view it as a positive sign that CISOs feel they are being listened to by senior management and that their recommendations are, for the most part, being considered and implemented. However, that has not always been the case in the past."

CISOs reported in the survey that there were still an abundance of issues that agencies must address and over the past year, some of their needs have begun to be met.

For instance, (ISC)^2 noted that CISOs "strongly favor(ed) a shift from compliance reporting to continuous monitoring, as well as the imposition of stricter security requirements during the acquisition of all major IT systems." And in May of this year, the U.S. House of Representatives moved to do just that by passing the National Defense Authorization Act. The legislation contains an amendment that would move agencies away from cumbersome paper-based compliance reports to continuous monitoring through a Web-based gateway.

CISOs in the (ISC)^2 report also expressed the need for "more resources and even more senior buy-in than they're currently getting to accomplish their mission." The proposed FISMA overhaul in part addresses the latter, giving CISOs greater latitude in gathering data from different departments and bureaus within their agencies.

And, of course, acquiring the proper resources, be it technology or people, has been a struggle against a tight budget for most CISOs. In the 1105 Government Information Group survey, 50 percent of the respondents said they expected to hire security personnel in the next 12 months. But many said they would turn to contract workers. The (ISC)^2 respondents noted that they seek workers with "experience, professional certifications and communication skills."

The Comprehensive National Cybersecurity Initiative 2 (CNCI2) announced this spring will focus on training and education and the creation of educational tracks and degree programs to turn out security professionals. In addition, a number of measures in that initiative will coordinate and manage "the federal enterprise network as a single network enterprise." By understanding and coordinating security initiatives across agencies, the government can identify the points of vulnerability, recommend where agencies need to take action and stimulate the use of shared resources.

Most CISOs in the (ISC)^2 survey claimed to be satisfied with their jobs. But while they note that they are more influential than ever before, they have a long way to go. According to the study, "76 percent of CISOs report to the agency Chief Information Officer, but none to the Chief Operating Officer, the Chief Financial Officer or the Chief Risk Officer, which CISOs believe limits their overall effectiveness." ❑