West Texas Cyber Security Consortium

GOVERNMENT IT REPORT

White House Tilts Toward Public-Private Cybersecurity Cooperation

By John K. Higgins
E-Commerce Times
Part of the ECT News Network
06/23/14 5:00 AM PT

Despite the administration's leaning toward a voluntary approach, legislation of some sort may be necessary to bring the private sector completely on board for a national, government-industry program to prevent cyberattacks or deal with them once under way. The trick will be for Congress to craft a bill that provides incentives for business cooperation while minimizing burdensome regulation.

The Obama administration and the private sector -- often at odds over the regulation of everything from telecom issues to software protection to the environment -- apparently agree that a major issue dealing with cybersecurity should be addressed on a cooperative basis, largely free of federal regulation.

The White House signaled its tilt toward a cooperative and voluntary approach for protecting "critical infrastructure" assets from cyberattacks and breaches in a notice issued last month by cybersecurity coordinator Michael Daniel.

The major conclusion of an administration study of executive branch agencies was that the study "supports our current voluntary approach to address cyber risk," Daniel said his post. "The administration has determined that existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information."

That commentary should not be taken as an administration move to entirely jettison cybersecurity regulation, of course. Its thrust was that no additional or new regulations were necessary. Existing regulatory authorities that affect cybersecurity still could take action if the government deemed it necessary to do so.

By and large, Daniel's comments were received as both significant and appropriate.

"While others are still toying with antiquated regulatory models to address this issue, the administration has charted a new and visionary course through the President's 2013 executive order on cybersecurity," said Larry Clinton, president of the Internet Security Alliance.

Daniel's recent commentary, he said, "is another welcome step in the right direction." ISA members include GE, Vodaphone, Northrup Grumman and Fidelity Investments.

"We have maintained all along that a static, government-centric regulatory model is not appropriate. Information technology changes too rapidly -- and frankly, so does the technology of hackers and others who commit these attacks," Clinton told the E-Commerce Times.

Report Minimizes Regulation

As part of a 2013 executive order and the adoption earlier this year of cybersecurity approach developed through the National Institutes of Technology, known as the "NIST Framework," the administration examined three major agencies regarding cybersecurity: the Department of Homeland Security, the Department of Health and Human Services, and the Environmental Protection Agency.

The review covered such critical infrastructure components as water, chemical hazards, food and medical supplies and services, and transportation. Each agency concluded that its existing authorities were adequate to meet the goals of the NIST Framework, and that voluntary and cooperative programs with the private sector were preferable to an exclusively regulatory approach.

The administration's policy was limited to implementation by agencies within the executive branch, and independent agencies such as the Nuclear Regulatory Commission or the Securities and Exchange Commission were free to take their own approaches to cybersecurity, Daniels noted.

"While those agencies have some leeway, there is a good chance the White House approach will serve as guidance to them as well. The Daniels blog and the executive order essentially

puts the administration in the role of a 'thought leader' to emphasize a collaborative approach," Clinton said.

"Certainly, the language in the White House statement is encouraging in terms of minimizing regulation, but you still have to realize that agencies have a wide breadth of current authority they could implement," David Inserra, research associate at the Heritage Foundation, told the E-Commerce Times.

Liability Protection Top Issue

The White House statement could put a damper on legislation that might result in additional regulation related to cybersecurity issues.

"At the very least, the administration's position would provide ammunition for opponents of any legislation that appears to be too heavy handed," Inserra said.

"Legislation which focuses on a regulatory approach is very unlikely to gain traction because of the administration's position," said Clinton.

Nonetheless, legislation of some sort may be necessary to bring the private sector completely on board for a national, government-industry program to prevent cyberattacks or deal with them once under way. The trick will be for Congress to craft a bill that provides incentives for business cooperation -- especially in sharing cyberincursion information -- but that minimizes burdensome regulation.

"The big issue still is liability reform," Inserra said. Businesses want to legally ensure that disclosure of cyber information to the government or within the business community will not trigger violations of various laws related to such disclosures."

The House last year approved a bill that includes such protections. The Cyber Information Sharing and Protection Act, or CISPA, which was passed by a 288-127 vote, addresses a variety of circumstances related to the handling of cybersecurity information. These include privacy protections, the elimination of any competitive advantages in the sharing of cyberdata, and liability protection for entities in the private sector.

The House bill "prohibits a civil or criminal cause of action against a protected entity, a self-protected entity, or a cybersecurity provider acting in good faith," according to the Congressional Research Service.

Legislation Still Necessary?

The Senate Intelligence Committee is working on a similar measure. Recently, Sen. Saxby Chambliss, R-Ga., the ranking Republican on the committee, said he was optimistic about enactment of cybersecurity information sharing legislation.

Chambliss and committee chair Sen. Diane Feinstein, D-Calif., "are currently working out some differences in their draft legislation related to the language in the bill on liability protection for companies that participate in information-sharing with the federal government," said law firm Squire Patton Boggs.

The IT community is maintaining a close watch on the legislative front.

"The protection of the networks that we rely upon for economic stability, national security and public safety against cyberthreats is a shared responsibility," Linda Moore, president and CEO of TechNet, told the E-Commerce Times. TechNet represents key Internet players such as Apple, Google, Intel and Cisco.

"An effective approach to cybersecurity requires sustained collaboration between public entities and the private sector in order to identify threats, vulnerabilities and consequences, and to manage the risks to American's health, safety and security," she said.

"TechNet is gratified the Senate continues to negotiate on cybersecurity and is supportive of a legislative approach that removes legal barriers and disincentives that prevent the sharing of timely threat information with those who are best positioned to act," Moore added.

In addition to private sector liability relief, there are several measures that could be used to further encourage better cybersecurity without cost to federal agencies, INA's Clinton noted. These include better use of private insurance, fast-track permitting, and patent approval processes for "good actors."

"We need to be even more aggressive in developing these incentive mechanisms," he said, "to address a vast and growing cyberthreat." ECT

John K. Higgins is a career business writer, with broad experience for a major publisher in a wide range of topics including energy, finance, environment and government policy. In his current freelance role, he

reports mainly on government information technology issues for ECT News Network.

http://www.technewsworld.com/story/80633.html