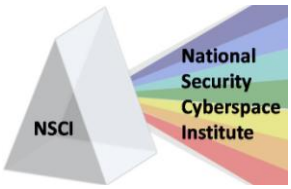

A Review of the Cybersecurity Legislative Proposal

Kathryn Stephens, NSCI
June 15, 2011

Overview

On May 12th, the Obama administration released its Cybersecurity Legislative Proposal which aims to provide guidance to Congress on several key cybersecurity legislative issues. The proposal is intended to bring together 50 cyber-related bills that were introduced in the last session of Congress, and focuses on "improving cybersecurity for the American people, our Nation's critical infrastructure, and the Federal Government's own network and computers."[1]

Some security experts have said the proposal does not take on tough cybersecurity decisions, and that the issues addressed in the proposal are not new issues. Others feel the proposal lacks the teeth or authority to cause effective change in current cyber legislation. The proposal does succeed in addressing civil liberties and privacy issues that can affect information sharing and data breach notification, and also better organizes cybersecurity responsibilities within DHS. The proposal also takes the first steps to toughen legislation that could help discourage cyber criminals. That said, the proposal fails to address many of the core issues at the heart of actually improving cybersecurity.

What does the legislative proposal address? What is being recommended?

Penalties for Cyber Crime

The first section of the cybersecurity legislative proposal discusses the need for harsher penalties for computer criminals. The proposal recommends that The Computer Fraud and Abuse Act be updated to include a mandatory minimum penalty for cyber-attacks, even those attacks that are thwarted. Harsher penalties would also be imposed when attacks target or damage critical infrastructure systems. The proposal also recommends adding cyber offenses to the Racketeering Influenced and Corrupt Organizations Act (RICO), which currently does not apply to cyber crimes. This would bring harsher penalties for organized crime groups that are increasingly committing online crime. In addition to these amendments, the proposal synchronizes computer crime with other crimes, and sets mandatory minimum prison sentences for cyber intrusions. Harsher penalties and minimum prison time may help discourage cyber criminals who currently have little risk of ever being found out or face minimal penalties for attempted computer crimes.

However, these increased penalties for cyber criminals, although important, will most likely not have much effect on the overall security of cyberspace. Cybersecurity has very complex legal issues, including how to coordinate legal penalties with other nations, how to enforce cyber crime penalties on criminals that can operate through borders and usually with complete anonymity, and how to attribute cyber crimes when they are detected. Although these guidelines are much needed, and will at least send a message to criminals who engage in cyber crime, they are reactionary and do little to help prevent cyber-attacks or address the frequently discussed challenge of attribution (e.g. knowing who is attempting / conducting the attack), a prerequisite for imposing penalties.

[1] "FACT SHEET: Cybersecurity Legislative Proposal." *The White House*. 12 May 2011. Web. 13 May 2011. <http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>.

Data Breach Notification

The cybersecurity legislative proposal also discusses new guidelines for data breach notification. The requirements specifically target organizations that handle the personal information of at least 10,000 individuals a year. These organizations would be required to notify potential victims in the event of a breach within 60 days, although extensions could be granted by the Federal Trade Commission for further investigation or if the FBI decides that notification would interfere with an investigation. Companies would be required to notify the Secret Service, FTC and FBI of all data breaches, and notification requirements would be enforced by the FTC.[2]

There are currently 47 different state laws that address notification requirements when personally identifiable information has been lost, stolen or exposed. The proposal aims to replace these individual laws in order to streamline and standardize the notification process. While this specific section of the proposal does not inherently make cyber more secure or reliable, national data breach notification regulations may help to protect computer users who can take steps to better protect their personal information and prevent fraud or identity theft.

In addition to providing guidance on notifying individual users, the proposal also addresses information sharing with industry, states, and local governments who may identify cyber threats or incidents, but are unsure about whether they can share information with the Federal Government. The proposal encourages businesses, state and local governments to share information with the Department of Homeland Security, and also provides privacy oversight to ensure that voluntarily shared information does not violate privacy and civil liberties. This is a positive step, since privacy concerns often prevent the private sector from sharing cyber breach information with the government.

Rep. Melvin Watt, D-NC, says that the proposal will grant immunity to companies that cooperate with federal investigations, similar to the immunity given to telecom companies that participated in warrantless wiretapping after 9/11. According to Watt, “these companies could then do something that’s unconstitutional just because you (the government) say it’s not,” and that “people get very uncomfortable with the idea that the government can just call up someone, demand information, and then provide them immunity.” Rep. Darrell Issa, R-Calif., says that the courts should be more involved in deciding when to grant immunity to private companies in order to keep the executive branch in check. [3]

Leslie Harris, president and CEO of the Center for Democracy and Technology (CDT) says that the proposal trumps previous limits on government access to private data in the Wiretap Act, the Electronic Communications Privacy Act, and other laws. According to Harris, the Obama proposal would “allow private organizations to share vast amounts of information with DHS” and would also allow DHS to request information in order to implement cyber programs. Rep. Watt says the proposal basically says

[2] Jackson, William. "DHS Rules in White House Cyber Plan." *Federal Computer Week*. 13 May 2011. Web. 13 May 2011. <http://fcw.com/articles/2011/05/13/white-house-cyber-plan-puts-dhs-in-charge.aspx>.
[3] Smith, Josh. "House Panel Worries That Obama Cybersecurity Plan Could Open Door to Abuse." NationalJournal.com. 25 May 2011. Web. 30 May 2011. <http://www.nationaljournal.com/tech/house-panel-worries-that-obama-cybersecurity-plan-could-open-door-to-abuse-20110525>.

that if private organizations do what they are asked to do, they are guaranteed immunity from any kind of liability. [4]

DHS Cybersecurity Authority and Information Sharing

The legislative proposal also reassigns certain infrastructure protection responsibilities under the Homeland Security Act of 2002 to the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity and other related programs. The proposal formalizes DHS's current role in managing cyber security for the Federal Government's civilian computers and networks and allows DHS to quickly help a private-sector company, state, or local government that asks for help. It also clarifies the type of assistance that DHS can provide to a requesting organization.

The proposal will require DHS to work with industry in identifying core critical-infrastructure operators and prioritizing current cyber threats and vulnerabilities. The core critical-infrastructure operators would be in charge of developing their own plans for addressing cyber threats, which would be evaluated by a third-party, commercial auditor. The proposal gives DHS the authority to modify the core critical-infrastructure operator's plans, or impose its own program by collaborating with the National Institute of Standards and Technology.[5]

The proposal also grants DHS more authority and oversight of federal systems. DHS's authority to oversee intrusion prevention systems for all Federal Executive Branch civilian computers is made permanent. These systems will be implemented by Internet Service Providers, and provisions from the legislative proposal include strong privacy and civil liberties protections, congressional reporting requirements and an annual certification process for intrusion prevention systems. DHS would also be in charge of conducting risk assessments for federal systems, remote and on-site technical assistance, ensuring situational awareness across federal systems, and testing and evaluating federal information security improvements.

The Defense Department would retain oversight of the dot-mil domain, and would work closely with DHS to protect cyberspace. Robert J. Butler, the deputy assistant secretary of defense for cyber policy, recently testified before the Senate Committee on Homeland Security and Governmental Affairs about the Obama proposal, and said that protecting national computer networks would require a "whole of government approach" that includes coordination at US Cyber Command and the National Security Agency. [6]

The proposal basically gives DHS formal oversight of cybersecurity operations within civilian federal agencies, but DHS has already been performing this role since last summer. The changes listed in the proposal are nothing new for DHS; the guidelines from the legislative proposal only serve to formalize

---

[4] Gross, Grant. "Lawmakers Question Obama Cybersecurity Proposal." Computerworld. 25 May 2011. Web. 30 May 2011. <http://www.computerworld.com/s/article/9217060/Lawmakers_question_Obama_cybersecurity_proposal>.
[5] Jackson, William. "Obama Cybersecurity Plan Ready for Congress." *Federal Computer Week*. 12 May 2011. Web. 13 May 2011. <http://fcw.com/articles/2011/05/12/white-house-cybersecurity-proposal.aspx>.
[6] "Pentagon to Help Protect U.S. Cyber Assets, Infrastructure." *Homeland Security News Wire*. 26 May 2011. Web. 30 May 2011. <http://www.homelandsecuritynewswire.com/pentagon-help-protect-us-cyber-assets-infrastructure>.

DHS responsibilities.[7] Critics of the new legislative proposal also say that increased information sharing between the public and private sectors is "nothing new." IT analyst Richard Stiennon says, "That's what US-CERT was set up for. No vision here."[8]

The proposal will undoubtedly be criticized for giving DHS the authority to impose government mandates on private sector organizations, rather than allowing a voluntary participation program, which could delay the approval of cybersecurity legislation.[9] Still, any attempt to clarify cyber responsibilities is a positive step towards better security and oversight.

Jeffrey Carr, founder and CEO of Taia Global, says that the proposal's recommendations for critical infrastructure protection predictably have "no bite." In a May 15 blog post, Carr writes that if a critical infrastructure operator does not comply with federal cybersecurity requirements, they would only "get a stern talking-to," "possibly get some publicity," or "be subject to some other unidentified action." The operator would not be shut down for non-compliance, fined, held financially responsible in the event of an attack, or otherwise be told what to do. Using the example of a power plant, Carr points out that the federal government regulates the construction of every aspect of the plant except for the protection of its networks, which Carr calls irrational and irresponsible. "Compliance cannot be voluntary or somebody doesn't know what 'critical' means."[10]

Senator Susan Collins, R-Maine, points out that the evaluation of a private company's cybersecurity plans would be publicly accessible, which could make cyberspace even less secure by giving our cybercriminals "a roadmap on how to attack our critical infrastructure." [11]

In order to actually help improve cybersecurity for the private sector, the proposal would have to be clearer on what DHS (and DoD) can and cannot do, instead of granting DHS broad but poorly-defined authorities. Larry Clinton, president of the Internet Security Alliance, says the proposal is disappointing when compared with the President's 2009 cybersecurity policy statement, because DHS is not given the authority to shut down private companies that do not comply with federal objectives, but DHS is given authority to take "other action as may be appropriate." This lack of clarity and actual authority will not help to secure cyberspace. Clinton points out that the President was "far wiser on this issue when he published the 2009 Cyber Space Policy Review, which in fact called for more incentives, including procurement and tax and liability policies" which are not included at all in the new proposal. [12]

---

[7] Sternstein, Aliya. "White House Sends Congress a Long-awaited Cybersecurity Proposal - Nextgov." *Nextgov.com*. 12 May 2011. Web. 13 May 2011. <http://www.nextgov.com/nextgov/ng_20110512_3812.php>.
[8] "Obama Pushes Cybersecurity Plan." *VietNetworks.org*. 15 May 2011. Web. 18 May 2011. <http://vietnetworks.org/software/obama-pushes-cybersecurity-plan.html>.
[9] "White House Reveals Refurbished Cybersecurity Plan." *Military.com*. 13 May 2011. Web. 13 May 2011. <http://www.military.com/news/article/white-house-reveals-refurbished-cybersecurity-plan.html>.
[10] Carr, Jeffrey. "The President's Cybersecurity Legislative Proposal Has No Teeth." *Digital Dao*. 15 May 2011. Web. 18 May 2011. <http://jeffreycarr.blogspot.com/2011/05/presidents-cybersecurity-legislative.html>.
[11] Sternstein 05/23/2011, Aliya. "Obama Cybersecurity Enforcement Plan Could Backfire, Senator Warns." Nextgov.com. 23 May 2011. Web. 31 May 2011. <http://www.nextgov.com/nextgov/ng_20110523_3112.php>.
[12] Higgins, John K. "Business Groups Give Thumbs Sideways to Obama's Cybersecurity Plan." *TechNewsWorld*. 19 May 2011. Web. 20 May 2011. <http://www.technewsworld.com/story/72491.html>.

The federal government will only be able to impact cybersecurity by proposing concrete, authoritative policies on industry and critical infrastructure oversight. The current proposal will likely lead to "further conversations," but will not be enough on its own to improve cyber policy for industry and critical infrastructure operators. Experts seem to agree there must be a balance of regulations and incentives in order to improve cybersecurity for the private sector.

The President, so far, maintains largely a hands-off policy on the creation of government-backed regulation and business incentives, which has discouraged industry from investing more in cybersecurity. The legislative proposal should have included tax credits for information security investment and research, research funding, reasonable immunity for companies that meet industry standards, exemptions for companies that develop collaborative cybersecurity programs, federal enforcement of industry standards, increased funding for enforcement, and perhaps clarification regarding the Federal Trade Commission's responsibility.

Amendments to Federal Information Security Management Act of 2002

In addition to clarifying DHS's role in managing cybersecurity for Federal Government civilian computers and networks, the administration's proposal also updates the Federal Information Security Management Act (FISMA). The proposal shifts FISMA responsibility from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) to DHS, but does not actually reform FISMA. This move could help the implementation of FISMA policies, which has historically been a "paperwork exercise" since no one at OMB or NIST knew how the attacks were occurring. The idea seems to be that DHS will be able to help FISMA implementation by providing attack information and best practices for organizations struggling with compliance. The Federal Government hopes the move would provide organizations with a shared source of expertise in the Department of Homeland Security.

Alan Paller, Research Director at the SANS Institute, said the FISMA upgrade included crucial details that are "central to making the government lead by example" but also admitted "there are people who are going to think they needed to do a lot more."[13]

Personnel Authorities Related to Cybersecurity Positions

The federal proposal grants the Secretary of Homeland Security the authority to establish cybersecurity positions, set competitive pay, and provide additional compensation and benefits for cybersecurity employees. The Secretary would also have the authority to establish a scholarship program that would help employees obtain a degree or certificate in an information assurance discipline. The White House recognizes that the recruitment and retention of highly-qualified cybersecurity professionals is extremely competitive, and hopes to increase DHS flexibility in hiring, as well as allowing the government and private industry to exchange cyber experts so that both government and industry can learn from each other.[14] The proposal explains that DHS would be given the same flexibility the

[13] Vijayan, Jaikumar. "Little New in Obama Cybersecurity Proposal - Computerworld." *Computerworld*. 13 May 2011. Web. 13 May 2011. <http://www.computerworld.com/s/article/9216671/Little_new_in_Obama_cybersecurity_proposal?taxonomyId=82>.
[14] "FACT SHEET: Cybersecurity Legislative Proposal." *The White House*. 12 May 2011. Web. 13 May 2011. <http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>.

Pentagon currently has, which helps the Pentagon to rapidly hire skilled professionals at competitive salary levels.[15]

There is no question there is a shortage of properly trained and certified cybersecurity workers in the federal government. Jim Gosler, a fellow at Sandia National Laboratories and the founding director of the CIA's information technology office, says the federal government needs "10,000 to 30,000" skilled cyber workers, although the government currently only has about 1,000 with the right skill sets.[16] The federal government must revise its hiring processes if they are serious about filling cybersecurity positions with government employees.

The government must also decide which certifications or degrees are most desired in order to classify a worker as highly-skilled or trained. Most certifications require the worker to only pass a test or complete a check list of skills, which does not always mean the employee has mastered a technical skill effectively. We need more concrete guidelines on what technical skills, degrees, certifications and experience are desired, and not another broad, vague call for skilled professionals.

Preventing Restrictions on Data Center Locations

In an effort to promote efficiency and innovation, the proposal prevents States from passing laws or adopting regulations that require a data center be located in a specific state as a condition of doing business. The Federal Government has long been a supporter of cloud computing which, according to the White House Cybersecurity Legislative Proposal, can "reduce costs, increase security, and help the government take advantage of the latest private-sector innovations." The proposal claims passing laws that require data centers to be in a specific state would cripple the government's ability to keep up with private sector innovation.[17] It is unclear how this section of the proposal will improve cyber security or reliability. The guidelines may indeed be needed since keeping competition and availability of cloud computing services available to the federal government can reduce costs and help the government take advantage of private sector innovations. However, this section of the legislative proposal does not have much effect on the core issues of cyber security.

What is missing from the cybersecurity legislative proposal?

A common criticism of the legislative proposal is that the plan fails to address some key cybersecurity issues for which Congress has requested guidance "The proposal is silent on several sticking points, including cyberwarfare, classified information and the criteria for so-called critical infrastructure." Another criticism concerns the failure to mention an Internet kill switch that would allow the president to shut down the Internet during cyber emergencies.[18] White House officials claim the president already

[15] Sternstein, Aliya. "White House Sends Congress a Long-awaited Cybersecurity Proposal - Nextgov." *Nextgov.com*. 12 May 2011. Web. 13 May 2011. <http://www.nextgov.com/nextgov/ng_20110512_3812.php>.
[16] Schwartz, Matthew. "Feds Desperate to Hire Information Security Pros." *Dice News*. 23 Nov. 2010. Web. 18 May 2011. <http://career-resources.dice.com/articles/content/entry/feds_desperate_to_hire_information>.
[17] "FACT SHEET: Cybersecurity Legislative Proposal." *The White House*. 12 May 2011. Web. 13 May 2011. <http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal>.
[18] Sternstein, Aliya. "White House Sends Congress a Long-awaited Cybersecurity Proposal - Nextgov." *Nextgov.com*. 12 May 2011. Web. 13 May 2011. <http://www.nextgov.com/nextgov/ng_20110512_3812.php>.

has sufficient emergency authority to act under existing rules, which is why no specific authority was outlined in the federal proposal.[19]

Maine Senator Susan M. Collins points out the administration's proposal seems to rely on the Telecommunications Act of 1934, which would give the president broad authority, including the authority to shut down the Internet. Senator Collins and Connecticut Senator Joe Lieberman have both said that rather than relying on outdated legislation, new legislation should be passed that provide clear specific guidance on executive branch powers to regulate Internet traffic. The Senators say debate over new legislation is not concerned with whether or not to create an actual mechanism that could shut off the Internet, but would provide guidelines for who can limit Internet accessibility and under what circumstances. [20]

Philip R. Reitinger, deputy undersecretary for the DHS National Protection and Programs Directorate, says "the 1934 law was not designed for the current environment" but the Obama administration would "use the authority that it brings to bear in the right way." Reitinger also says the president's proposal is not a bill, but is the administration's input into the legislative process requiring further negotiation.[21]

Security experts also argue that while the proposal did outline civilian agencies' roles in protecting computer networks, it left out guidance on national security networks that carry classified information. Lawmakers and agencies have been debating whether the Defense Department or the Homeland Security Department should be responsible for actually responding to cyberattacks.[22] Another surprising issue that was left out of the legislative proposal was the issue of the formal establishment of an executive branch cybersecurity officer. Howard Schmidt was named by President Obama to be the White House cybersecurity coordinator, but the position does not require Senate approval, although many lawmakers believe it should.[23]

Do the included recommendations make cyber more secure?

Will the Federal Cybersecurity Legislative Proposal make cyberspace more secure? Some security experts say no. Richard Stiennon, an analyst at IT Harvest, says that nothing in the proposal will "move the needle significantly on cybersecurity." Stiennon points out that Congress has been working on a data breach notification law that would bring together all of the different state laws since 2004, but the task is still not complete. Stiennon also points out that threats are continuing to evolve, while we continue to focus on implementing outdated protections like IPS systems. Finally, Stiennon says the federal

[19] Jackson, William. "Obama Cybersecurity Plan Ready for Congress." *Federal Computer Week*. 12 May 2011. Web. 13 May 2011. <http://fcw.com/articles/2011/05/12/white-house-cybersecurity-proposal.aspx>.
[20] "Internet Kill Switch Option Actively Debated by Senate." Infosec Island. 24 May 2011. Web. 30 May 2011. <https://www.infosecisland.com/blogview/13966-Internet-Kill-Switch-Option-Actively-Debated-by-Senate.html>.
[21] Jackson, William. "White House Proposal Includes Internet Kill Switch, Senators Warn." *Federal Computer Week*. 24 May 2011. Web. 30 May 2011. <http://fcw.com/articles/2011/05/23/cybersecurity-plan-hearing-kill-switch-returns.aspx?admgarea=TC_HLS>.
[22] Sternstein, Aliya. "White House Cyber Proposal Excludes Classified Systems." *NextGov.com*. 11 May 2011. Web. 13 May 2011. <http://cybersecurityreport.nextgov.com/2011/05/white_house_cyber_proposal_excludes_classified_systems.php>.
[23] Jackson, William. "DHS Rules in White House Cyber Plan." *Federal Computer Week*. 13 May 2011. Web. 13 May 2011. <http://fcw.com/articles/2011/05/13/white-house-cyber-plan-puts-dhs-in-charge.aspx>.

government will likely receive criticism for becoming more involved in helping private sector companies with cybersecurity rather than just focusing on protecting the government.[24]

Critics also feel the proposal should have included more urgent measures, since House and Senate committees have been working on cyber security legislation for the past two years, waiting on the Obama administration to provide input.[25] Former senior Homeland Security official Stewart Baker says the White House proposal has "little teeth" and "no sense of urgency." Baker explains the proposal does not require critical infrastructure security measure evaluation for at least a few years.[26]

Some lawmakers, however, believe the proposal is a valuable step towards better securing cyberspace. Commerce Committee Chairman John D. Rockefeller, D-W.Va., called the proposal a "strong plan to better protect our nation from the growing cyber threat" and said he looks forward to working with the Obama administration to pass a comprehensive cybersecurity bill this year. Ranking member Sen. Olympia Snowe, R-Maine, pointed out the guidance from the White House was long overdue, but said she agreed with the proposal's objectives, especially those pertaining to public-private partnership.[27]

Security experts seem to agree that some guidance from the cybersecurity legislative proposal may make cyberspace more secure. One of the biggest changes included in the proposal is the federal data breach requirements, which would improve breach notification processes dramatically by replacing the 47 different state laws. A Commerce Department official says that "a nationwide standard for data-breach notification would make compliance much easier."[28] The proposal's requirement that critical infrastructure operators identify key threats and then prepare a cybersecurity plan would almost certainly help to better protect our nation's critical infrastructure, although some worry the proposal will spark a debate between those who think the private sector should be able to voluntarily participate rather than be forced to comply with mandates from DHS. Joseph Lazzarotti, a partner with law firm Jackson Lewis L.L.P. in White Plains, N.Y., says businesses should be provided with cybersecurity resources rather than forced to abide by government imposed guidelines.[29]

Security analyst Jon Oltsik says although he is encouraged that the Obama administration has released some legislative guidance on cybersecurity, he is still not convinced Washington will respond quickly and effectively to better secure cyberspace. Oltsik points out that the Cybersecurity and Information

[24] Vijayan, Jaikumar. "Little New in Obama Cybersecurity Proposal - Computerworld." *Computerworld*. 13 May 2011. Web. 13 May 2011. <http://www.computerworld.com/s/article/9216671/Little_new_in_Obama_cybersecurity_proposal?taxonomyId=82>.
[25] Ashford, Warwick. "White House Proposes Cyber Network Security Legislation." *ComputerWeekly.com*. 13 May 2011. Web. 13 May 2011. <http://www.computerweekly.com/Articles/2011/05/13/246646/White-House-proposes-cyber-network-security-legislation.htm>.
[26] "White House Reveals Refurbished Cybersecurity Plan." *Military.com*. 13 May 2011. Web. 13 May 2011. <http://www.military.com/news/article/white-house-reveals-refurbished-cybersecurity-plan.html>.
[27] Sternstein, Aliya. "White House Sends Congress a Long-awaited Cybersecurity Proposal - Nextgov." *Nextgov.com*. 12 May 2011. Web. 13 May 2011. <http://www.nextgov.com/nextgov/ng_20110512_3812.php>.
[28] Jackson, William. "Obama Cybersecurity Plan Ready for Congress." *Federal Computer Week*. 12 May 2011. Web. 13 May 2011. <http://fcw.com/articles/2011/05/12/white-house-cybersecurity-proposal.aspx>.
[29] Greenwald, Judy. "Obama Administration Proposes Cyber Security Protections." *Business Insurance*. 12 May 2011. Web. 13 May 2011. <http://www.businessinsurance.com/apps/pbcs.dll/article?AID=/20110512/NEWS/110519978>.

Freedom Act has been stuck in the Senate for several months already, along with other bills from Senators Rockefeller (D-W.Va.) and Snowe (R-Maine), Congressman Langevin (D-R.I.) and others.[30]

It would appear the Obama administration is consistently getting an "A for effort" in cybersecurity matters, but politicians and business groups are less convinced on the details of cybersecurity program specifics. In a recent TechNewsWorld article, author John K. Higgins said "the anticipated momentum for Congressional action related to the administration's proposals may be elusive. Instead, there may be an all-too-familiar logjam, as both substantive and political issues slow down the legislative process." [31] Security expert Kevin Coleman says while this guidance has been a long time coming, "the devil is in the details and the administration's vision is far from detailed." Coleman says details from 50 different cybersecurity legislative pieces will be added to the Obama administration proposal over the next several months, and much more information is needed. [32]

[30] Oltsik, Jon. "Good News and Bad News On Obama Cybersecurity Legislative Proposal Letter." *Network World*. 17 May 2011. Web. 18 May 2011. <http://www.networkworld.com/community/node/73892>.
[31] Higgins, John K. "Business Groups Give Thumbs Sideways to Obama's Cybersecurity Plan." *TechNewsWorld*. 19 May 2011. Web. 20 May 2011. <http://www.technewsworld.com/story/72491.html>.
[32] Coleman, Kevin. "President Obama's Cyber Security Plan." *Defense Tech*. 20 May 2011. Web. 30 May 2011. <http://defensetech.org/2011/05/20/president-obama's-cyber-security-plan/>.