United States Senate
Committee on Homeland Security and Governmental Affairs
Senator Joseph I. Lieberman, Chairman
Senator Susan M. Collins, Ranking Member

What Key Groups and Experts Are Saying About the Lieberman, Collins, Carper Cybersecurity Bill

Businesses

Microsoft

Fred S. Humphries, Jr., Vice President of U.S. Government Affairs says:

"Your bill…demonstrates a deep understanding of the challenges that the nation faces in cyberspace, and provides a much needed structure and process to address those issues… The government, as a public policy entity, is responsible for protecting public safety, as well as economic and national security, and the United States must develop and implement a comprehensive strategy to address the full spectrum of risks presented in cyberspace… If enacted, S. 3480 will help to strengthen the appropriate roles of government in building and implementing a national strategy and also in protecting its own enterprise. We strongly support the intended outcomes of this legislation and key provisions it offers to advance cyber security."

Verizon

Peter Davidson, Senior Vice President of Federal Government Relations says:

"Threats in cyberspace are real, and the Lieberman-Collins-Carper bill would help the nation to address them more effectively. As the operator of complex global data networks, Verizon welcomes legislation like this that creates a cooperative, public-private approach to cyber security. We stand ready to assist the government in its efforts to increase the security and resiliency of our nation's critical cyber networks."

McAfee

Dave DeWalt, Chief Executive Officer says:

"Senators Lieberman, Collins, and Carper must be commended for crafting a thoughtful cyber security reform bill that will help secure our Federal government and our nation's critical infrastructures. The Senators and their staffs have done an outstanding job of reaching out to the IT industry to get our feedback on this bill. McAfee looks forward to working with our colleagues in the IT industry and the sponsors of this bill to further refine language that addresses security standards, supply chain mandates, and critical infrastructure reporting requirements."

Symantec

Mark Bregman, Executive Vice President & Chief Technology Officer says:

"As the world's information security leader, Symantec would like to convey our support for the 'Protecting Cyberspace as a National Asset Act of 2010'. This

important legislation will enhance and modernize our nation's overall cyber security posture in order to safeguard our critical infrastructure from attack. The bill also importantly recognizes cybersecurity as a shared government and private sector responsibility which requires a coordinated strategy to detect, report and mitigate cyber incidents. We look forward to working with the Committee to help advance this important legislation."

Exelon Corporation

Steven T. Naumann, Vice President of Wholesale Market Development says:

"I applaud the committee for addressing what additional authority is needed to promote clarity and focus in response to imminent cyber security threat situations."

"Another important component is your legislation's narrow scope; it focuses appropriately on the need to protect truly critical assets. There is a security axiom that states: if you try to protect everything, you protect nothing. Put another way, the risk-based prioritization reflected in the proposed bill ensures both government and private sector resources are allocated wisely."

EMC Corporation

Art Coviello, Executive VP at EMC Corporation & President at RSA, and Dave Martin, Chief Security Officer at EMC Corporation say:

"EMC and RSA provide information infrastructure solutions to thousands of enterprises in the public and private sectors. Daily, we address the constantly evolving threats and risks in cyberspace. As a result, we are acutely aware not only of the cyber security challenges that organizations of all sizes face, but also of the resources, talent, innovative strategies, and vigilance required to effectively manage cyber risks. It is with this perspective that we thank you for crafting a comprehensive bill that incorporates a risk-based approach to protecting information infrastructure in both the public and private sectors."

Lieberman Software Corporation

Philip Lieberman, President says:

"I applaud the Lieberman-Collins bill S 3480 "Protecting Cyberspace as a National Asset Act of 2010" for having the courage to begin the process of securing cyberspace. There will be corrections, clarifications and improvements to the bill, as well as additional bills to provide more technical and legal prescriptive guidance and legal remedies.

Clearly, the utilities are not doing a great job in security and it would be great if the

government could force them to do the right thing. No doubt there is great political benefit to making a public example of the utilities for their lackluster implementation of security.

I can say from first-hand knowledge that when we try to sell utilities our security solutions for privileged identity management, we typically get rejected in favor of cheap, off-shore, inferior and potentially compromised solutions. It is clear that the utilities are on a suicide mission with respect to internal security and the government needs to force them to step up their game to be in line with the value of the resources they control. Rather than solve it in Lieberman-Collins, the legislature needs to craft specific legislation to wake up the utilities before they send us all into semi-permanent darkness when the US does something to irritate another government or hacker group with cyber warfare capabilities.

Let's do something, and make it even better via the legislative process. This legislation is a great starting point."

Current and Former Government Officials

Karen Evans, Former Administrator for E-Government and IT, Office of Management and Budget

"I am really excited about the introduction of this legislation especially as it relates to strengthening the authorities of DHS. It is necessary for the Director of the National Center for Cybersecurity and Communications to have the appropriate authorities to really make a difference and improve the security posture of the federal agencies and critical infrastructure and this bill does exactly that. I am especially excited with the inclusion of the workforce provisions such as the establishment of the cyber talent competitions and challenges. By addressing all aspects of the cyber security issue, the passage of this bill will really make a difference in reducing the overall risk to our federal agencies and critical infrastructure."

Stewart Baker, former Assistant Secretary for Policy at DHS and former General Counsel for NSA

"As we've come to expect from the bill's cosponsors, this is a careful and responsible bipartisan approach to a serious problem that could become a crisis at any time. It provides a comprehensive framework for addressing the problem and protecting our most critical infrastructure without forcing unnecessarily broad new mandates on an industry that contributes greatly to our economy's productivity."

Bob Gourley, Former Chief Technology Officer of the Defense Intelligence Agency (DIA)

"By ensuring the White House will have a Senate-confirmed Director, it will help underscore for the executive branch that this issue should be taken a bit more serious. Sounds like a prudent thing for the Congress to do… This office will have authority to lead across government. As a CTO with enterprise experience I respect this kind of position… Naming the NCCC as the focal point for coordination with the federal sector is also a solid move… As a CTO, I applaud the measures this Bill describes for removing artificial impediments to information sharing. Government and industry need trust-based relationships and unfortunately too many laws and behaviors that flow from those laws, like FOIA, have damaged those relationships. Addressing them head on is the right thing to do."

Philip Reitinger, Deputy Under Secretary, National Protection and Programs Directorate at the Department of Homeland Security

"DHS welcomes working with the Committee on strengthening the Department's ability to accomplish its cyber security mission—securing federal executive branch civilian systems and working with the private sector and federal sector-specific agencies to secure the nation's CIKR…Thank you again for your strong support of the Department, and for your dedication to improving cyber security. We look forward to working with you to strengthen efforts that are critical to the nation's security, bolster the Department's ability to combat terrorism and respond to emergencies and potential threats, and allow DHS to tackle its responsibilities to protect the nation and keep Americans safe."

Outside Groups

Internet Security Alliance

Larry Clinton, President and CEO says:

"The Internet Security Alliance (ISA) wishes to express its gratitude to you for calling attention to the severe and growing cyber security problems our nation faces by introducing S. 3480."

SANS Institute

Alan Paller, Director of Research says:

"Thursday [June 10] was a very good day for information security in government…The Senate began the process of transforming federal information security so that the U.S. government can lead by example in making America's computers and networks much safer than they are today."

"By enacting the legislation before you, with a few small amendments… Congress can immediately change the way the cyber-security game is played to the benefit not just of government, but of the economy and the American people."

"Your procurement and supply chain language is both important and innovative."

"The regulatory framework and the emergency measures you establish for the critical infrastructure is long overdue."

U.S. Chamber of Commerce

Ann Beauchesne, Vice President of National Security & Emergency Preparedness says:

"Cyber security threats are growing in scope and sophistication and causing significant challenges for businesses of all sizes… The Chamber is analyzing the bill and its impact on the business community. We look forward to continuing a productive dialogue with the committee to strengthen and protect the American economy."

Center for Democracy and Technology

Leslie Harris, President says:

"We thank Senators Lieberman, Collins and Carper for their leadership on cybersecurity and for the care that went into this complex, sweeping legislation…

The bill includes some important privacy protections for Internet communications that might be sought by DHS in connection with its cybersecurity mission and shared with intelligence and law enforcement agencies."

TechAmerica

Phillip J. Bond, President and CEO says:

"The bill provides for three specific and important elements of cybersecurity today: elevating cybersecurity in the White House and the Department of Homeland Security as well as in the federal agencies; updating federal information security management to reflect a risk-based approach with continuous monitoring; and bolstering the public-private partnership to incorporate collaboration at the earliest possible stage and on a continuing basis."

Intelligence and National Security Alliance (INSA)

Ellen E. McCarthy, President says:

"INSA's Cyber Security Council has been closely and actively studying the problems surrounding national cyber security for the past two years, to include supporting the White House 60-Day Review of Cyber Security. In their latest publication, Addressing Cyber Security through Public - Private Partnership, the Cyber Security Council calls for clear ownership of the problem and the creation of a central, responsible party within government with whom the private sector can interact and consult on security issues. We believe this legislation can and will create such a center and that it is a vital step forward in the effort to secure cyberspace and preserve American power and security."

Frances Fragos Townsend, Chairwoman of the INSA Board says:

"With this bill, the Senate has taken the lead in identifying cyber security needs and organizing the government to address them."

"The goal is to make a positive and meaningful contribution to the national security of the United States and this bill goes a long way towards achieving that goal."

The Professional Services Council (PSC)

Alan Chvotkin, Executive Vice President says:

"PSC strongly supports the leadership that both Chairman Lieberman and Ranking Member Collins have shown with this legislation. It addresses, and provides solutions for, a number of important federal Government issues relating to cyber security, including the appropriate focus on acquisition strategies, supply

chain management, information sharing and risk assessments ... We thank you for the opportunity to be engaged in the development of this important national policy and look forward to continuing to working further with you on it. PSC strongly urges your committee to act expeditiously to move a bill to the full Senate for its prompt consideration."

Alliance for Gray Market and Counterfeit Abatement (AGMA)

Scott C. Olsen, Chairman of AGMA Government Affairs Committee says:

"…we would like to congratulate you for the important steps you have taken to support the acquisition of authentic information technology by the federal government in S. 3480…Your provisions in this area, as part of Section 253, recognize the critical risk-mitigating effects that *authentic* IT has and will, we believe, encourage the federal government's acquisition professionals to place new levels of value on such projects. In so doing, the risks created by current acquisition practices --- which fail to emphasize the important benefits of authentic IT --- will be minimized."

Coalition for Government Procurement

Larry Allen, President says:

"I am writing to offer the Coalition's support of the Protecting Cyberspace as a National Asset Act of 2010 which enhances the security and resiliency of the cyber and communications infrastructure of the United States… A partnership between the private and public sector is necessary to ensure that the government remains up to date from a technology perspective… From a procurement perspective, the Coalition supports the notion that federal agencies should seek products and services that are secure. Information about a product's features as well as assurance that the supply chain is secure provides government customers with the information they need in order to purchase the right information technology goods and services to meet our nation's cyber security objectives."

News Stories

Protecting Cyberspace Act Gains Momentum

by Mickey McCarter
Homeland Security Today

Bill contains no 'Internet kill switch' as feared by critics

The Senate Homeland Security and Governmental Affairs Committee last week advanced a cybersecurity bill that, according to critics, contains a "kill switch" that would enable the President to turn off the Internet in the event of a cyber attack.

In reality, the bill contains no such provision but would in fact strengthen and extend congressional oversight and protections of the Internet in the event of an emergency while providing the White House and the Department of Homeland Security (DHS) with appropriate mechanisms to respond to an attack, the bill's sponsors replied.

Indeed, prior to the committee's vote Thursday on the Protecting Cyberspace as a National Asset Act of 2010 (S. 3480), Sens. Joseph Lieberman (I-Conn.), Susan Collins (R-Maine), and Tom Carper (D-Del.) defended their bill with a series of facts targeted at clearing up misconceptions and hyperbole directed at its contents.

The White House appears to prefer to use existing authorities to deal with cyber emergencies, although it has not released an official statement on the bill. Testifying on the bill in a June 15 hearing, top DHS cyber official Philip Reitinger indicated to the committee that the Obama administration would prefer to rely upon powers such as those contained in Section 706 of the Communications Act of 1934.

The Communications Act presently provides the President with undefined authorities to "cause the closing of any facility or station for wire communication" and "authorize the use of control of any such facility or station," the bills' sponsors stated in a June 23 fact sheet. The President can use this authority without notifying Congress and after the declaration of an emergency. The White House can extend the authority up to six months after a "state of threat of war" has passed.

The Protecting Cyberspace Act would curtail that power by allowing the White House to exercise limited authority over portions of the Internet for 30-day increments. The bill would direct the White House to limit disruptions to the Internet and prevent a government takeover of it, the senators said.

Congress would require as much advance notice as possible before declaring a cyber emergency, triggering the capability to isolate portions of the Internet to prevent the spread of a cyber attack. The White House could only extend this authority for six months before it must receive additional permission from Congress to use it further under the bill.

The private sector would have an opportunity to propose alternative measures to shutting down servers and networks owned and operated by affected companies. DHS would have the opportunity to approve these measures through a new National Center for Cybersecurity and Communications (NCCC), which the bill also would create.

Lieberman hailed passage of his bill in a June 24 statement, saying the legislation "would fundamentally reshape the way the federal government defends America's cyberspace."

"It takes a comprehensive, risk-based, and collaborative approach to addressing critical vulnerabilities in our own defenses. We believe our bill would go a long way toward improving the security of our government and private critical infrastructure, and therefore the security of the American people," he stated.

The homeland security committee referred the bill to the full Senate for consideration. In the House, Rep. Jane Harman (D-Calif.) introduced a companion bill (HR 5548), which was referred to the Oversight and Government Reform, Homeland Security, and Science and Technology June 16.

Lingering concerns

Despite the lack of an "Internet kill switch" in the bill, civil liberties organizations have expressed concerns that the Protecting Cyberspace Act would go too far to limit communications in the name of security.

The American Civil Liberties Union (ACLU), the Center for Democracy and Technology (CDT), and other organizations teamed up to express their concerns in a June 23 letter to the Senate Homeland Security and Governmental Affairs Committee.

In their letter, the organizations outlined concerns that the bill would provide the President with unspecified emergency power to protect the operations of critical infrastructure by isolating portions of it.

"While the bill makes it clear that it does not authorize electronic surveillance beyond that authorized in current law, we are concerned that the emergency actions that could be compelled could include shutting down or limiting Internet communications that might be carried over covered critical infrastructure systems," the letter said. "This section should be amended to articulate the specific emergency actions the NCCC can compel, and any applicable limits on those actions.

"It should also be amended to ensure that emergency measures undertaken do not unnecessarily disrupt Internet communications. The Internet is vital to free speech and free inquiry, and Americans rely on it every day to access and to convey information," the letter added.

The bill also should undergo an independent evaluation to determine any impact it may have on free speech, privacy, and civil liberties, the groups said.

Harry Reid (D-Nev.), the Senate majority leader, has stated support for moving forward a comprehensive cybersecurity bill, which could see the Protecting Cyberspace Act combined with other efforts such as those considered by the Senate Commerce Committee and the Senate Armed Services Committee.

The Protecting Cyberspace Act appears to be gaining support and momentum on its own, however, and the Senate could choose to consider the bill on its own.

Joe Lieberman And The Myth of The Internet Kill Switch

Megan Carpentier
TPMDC

It's no secret that Senator Joe Lieberman (I-CT) isn't the most popular guy in the Senate, or that his rather conservative positions on national security have left many people suspicious of his motives when it comes to national security legislation. So it should have come as no surprise when CNET chief political correspondent Declan McCullagh wrote that Lieberman intended to give the President the power of an "Internet kill switch" in the event of a national emergency -- and sparked an uproar.

But, surprising it was -- especially to Lieberman and his staff on the Senate Committee on Homeland Security and Government Affairs. They argued that, in fact, the bill limited the powers already invested in the President to shut down telecommunications providers. Leslie Phillips, the communications director for the committee, said, "The very purpose of this legislation is to replace the sledgehammer of the 1934 Communications Act with a scalpel." So, who is right?

A review of the 1934 Telecommunications Act (as amended in 1996) does indicate that the President has broad powers to simply shut off any and all regulated telecommunications if he deems it necessary for national security. Section 706 of the Act, entitled "War Emergency -- Powers of the President" says:

(c) Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense, may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States as prescribed by the Commission, and may cause the closing of any station for radio communication, or any device capable of emitting electromagnetic radiations between 10 kilocycles and 100,000 megacycles, which is suitable for use as a navigational aid beyond five miles, and the removal therefrom of its apparatus and equipment, or he may authorize the use or control of any such station or device and/or its apparatus and equipment, by any department of the Government under such regulations as he may prescribe upon Communications Act of 1934 just compensation to the owners. The authority granted to the President, under this subsection, to cause the closing of any station or device and the removal therefrom of its apparatus and equipment, or to authorize the use or control of any station or device and/or its apparatus and equipment, may be exercised in the Canal Zone.

(d) Upon proclamation by the President that there exists a state or threat of war involving the United States, the President, if he deems it necessary in the interest of the national security and defense, may, during a period ending not later than six months after the termination of such state or threat of war and not later than such earlier date as the Congress by concurrent resolution may designate, (1) suspend or amend the rules and regulations applicable to any or all facilities or stations for wire communication within the jurisdiction of the United States as prescribed by the Commission, (2) cause the closing of any facility or station for wire communication and the removal therefrom of its apparatus and equipment, or (3) authorize the use or control of any such facility or station and its apparatus and equipment by any department of the Government under such regulations as he may prescribe, upon just compensation to the owners.

In other words, as Phillips told us, the President already has an Internet kill switch: he can't shut off a website, but he can shut off any and all wireless or wired Internet access.

Lieberman's Protecting Cyberspace as a National Asset Act of 2010 (S. 3480) is, thankfully, somewhat more complex than that. It requires that owners of critical infrastructure, a definition that dates to the PATRIOT Act, work with the newly created director of the National Center for Cybersecurity and Communications within the

Department of Homeland Security, to develop a risk assessment and a plan to mitigate their risks in the case of a national cyber emergency. If an emergency is declared, that director will:

(A) immediately direct the owners and operators of covered critical infrastructure subject to the declaration under paragraph (1) to implement response plans required under section 248(b)(2)(C);

(B) develop and coordinate emergency measures or actions necessary to preserve the reliable operation, and mitigate or remediate the consequences of the potential disruption, of covered critical infrastructure;

(C) ensure that emergency measures or actions directed under this section represent the least disruptive means feasible to the operations of the covered critical infrastructure

None of those response plans expressly require that telecommunications providers develop a kill switch; in fact, the director is prohibited from requiring an critical infrastructure owner or operators from using any specific mechanism.

The owners and operators of covered critical infrastructure shall have flexibility to implement any security measure, or combination thereof, to satisfy the security performance requirements described in subparagraph (A) and the Director may not disapprove under this section any proposed security measures, or combination thereof, based on the presence or absence of any particular security measure if the proposed security measures, or combination thereof, satisfy the security performance requirements established by the Director under this section.

Phillips reiterated this point with TPMDC: "There is not a 'kill switch.'" When asked what measures might be envisioned by the legislation, she said, "A software patch, or a way to deny traffic from a certain country. All these measures were be developed with the private sector, not imposed on it."

In addition to the measures that allow companies to come up with their own ways to mitigate the risks to their companies (and customers) from cyber attacks, and the requirement that they use the least disruptive means possible and attempt to mitigate larger impacts, the legislation also only allows the President to impose the state of emergency for 30 days, with a potential extension of 30 days. Under current law, he is allowed to shut down any and all telecommunications infrastructure for as long as he likes.

McCullagh said, in his initial analysis, that "The legislation announced Thursday says that companies such as broadband providers, search engines, or software firms that the government selects 'shall immediately comply with any emergency measure or action developed' by the Department of Homeland Security." That is slightly misleading, as owners and operators of critical infrastructure have already been identified by the Department of Homeland Security as part of the PATRIOT Act and the 2002 Homeland Security Act.

Although the full list of pieces of critical infrastructure isn't available for download for obvious reasons, the membership of the Critical Infrastructure Partnership Advisory Council -- which is designed to give those owner-operators a chance to work closely with DHS when they are developing their regulations and assessing the ways to best protect critical infrastructure -- is publicly available. And, if gives a pretty comprehensive look at what, exactly, DHS considers "critical infrastructure."

There are 17 sector committees -- everything from chemical companies to nuclear facilities and shipping companies to dam operators. There is also one committee for communications infrastructure and another for

information technology. The Communications Committee and Information Technology Committee have some overlap in terms of membership, but the exclusively consist of Internet infrastructure providers, telecommunications companies, some hardware companies and software companies that work in the security area. They do not include search engines, news web sites or anything of the kind -- sorry, folks, the government just doesn't consider you "critical" enough.

Phillips told TPMDC, "This language was developed with the companies who would be affected by it... The Senator [Lieberman] discussed the bill with privacy experts, civil liberties experts, companies affected by it, the Administration and the House." She expressed a certain level of shock about the backlash, pointing us to the committee's statements of support, which includes quotes from McAfee and Symantec executives (both members of the DHS Information Technology Committee); from the Center for Democracy and Technology -- which gave a quote seemingly not in support of the bill to CNET; and from the regulation-hating U.S. Chamber of Commerce.

On the one hand, yes, it does appear that this gives the government power over marginally more companies than it has now: there are critical infrastructure owners and operators not covered by the 1934 law that would be required to come up with a plan to respond to cyber attacks that meets certain standards set by the government. On the other hand, the Emergency Broadcast System, which requires that all television and radio stations interrupt their programming with a loud buzzing noise and carry the emergency message from the government might become a thing of the past if owners and operators could find better (and less disruptive) ways to alert Americans that there is an emergency. And, regardless, the President would only have 30 days to impose the state of emergency with little oversight, and the companies would be required to be as minimally disruptive to the rest of us as possible in the emergency plans they develop.

The "kill switch," though, won't be coming to the underside of the President's desk anytime soon, though. In fact, Lieberman's people seem to be correct: their bill actually just takes it away. The bill, by the way, faces a committee mark-up on Wednesday.

Blogs

Obama Can't Turn Off the Internet

By Adam Ross
NextGov—Cybersecurity Report Blog

The sweeping cybersecurity bill from Sens. Joe Lieberman, I-Conn., Susan Collins, R-Maine, and Tom Carper, D-Del., has come under unfounded fire for giving government the authority to shut down Internet services during emergencies. For the life of me, I can't find where it says this in the bill.

In section 249, under "National Cyber Emergencies" there is nothing linking a presidential declaration of a national cyber emergency to a "kill switch" for turning off the Internet. It simply does not exist. In fact, the president already has the authority to shut down communications networks, but that authority has nothing to do with this bill. Rather, it's part of the 1934 Communications Act.

The criticism is just another poor attempt to divert attention away from the pieces of the legislation that really matter. For example, the shift from compliance by paper to continuous monitoring will save the federal government hundreds of millions of dollars annually. But you rarely see it reported by the media or the blogosphere.

Instead, both mediums continue to propagate lies that have been repeated hundreds of time and so are assumed true. The only authority S.3480 gives the president is to direct the ISPs to filter specific attack traffic or traffic from specific bad places.

The complaints you are hearing are just like the ones the automobile industry used when they didn't want to put seat belts in cars. The industry claimed that passengers would not be able to get the belts off quickly enough and would be burned to death in accidents.

Dirty politics won't be enough to sink what is a very good bill. This won't be a Harry and Louise situation. Once the bill makes it to the floor, it should have the support it needs to become law.

Editorials and Op-Eds

Need to protect U.S. from cyber attack is critical

By Anthony Amore
Security Brief Column
Boston Herald

Last week Senate Homeland Security Committee Chairman Joseph A. Lieberman (I-Conn.) introduced legislation granting the president authority to take "emergency measures" to protect the nation's critical infrastructure in the event of a cyber attack.

Formally titled the Protecting Cyberspace as a National Asset Act and co-sponsored by Sen. Susan M. Collins (R-Maine) and Sen. Thomas R. Carper (D-Del.), the bill is intended to prevent what Collins called a "cyber 9/11."

Lieberman added, "The government's efforts to secure cyber networks have been disjointed, understaffed and underfinanced."

No one can reasonably argue with such assessments, and that's particularly disheartening given that the United States took the lead in creating the Internet but is woefully behind in defending it. As former Director of National Intelligence Mike McConnell chillingly noted, "If we were in a cyber war today, the United States would lose."

In his book "Cyber War: The Next Threat to National Security and What to Do About It," former White House counterterrorism czar Richard A. Clarke, the first person to sound alarms about al-Qaeda, details how cyber attacks are being used and the nightmarish effect they could have on our nation unless we act now.

Clarke foresees major problems for our transportation system should the United States be hit. A large-scale cyber attack could grind trains to a halt and explode pipelines transporting critical fuel supplies. The U.S. air traffic control system, which relies on 1970s technology and has been the subject of sharp criticism for years, is especially vulnerable.

It's not hard for the most technologically ignorant person to understand the horrifying effects an attack on the air traffic control system would have on our safety and our economy.

The Lieberman-Collins-Carper bill goes to great lengths to protect privacy despite the powers it gives the presidency. It prohibits using its emergency measures to conduct new surveillance, and it has been lauded by the civil liberties-minded Center for Democracy and Technology for its emphasis on privacy protections.

Congress should waste no time in passing this measure. Hostile nations such as North Korea have been recruiting, training and employing hackers to wage cyber war. Pyongyang is suspected of waging a cyber attack against the U.S. government in 2009, disabling the Web servers of agencies including the Secret Service. It's time we shore up our defenses against this emerging, and very frightening, threat.

A cyber bill worth enacting

Federal Computer Week
By Wyatt Kash

We have routinely supported those who call for the overhaul of the Federal Information Security Management Act and highlight the need for more effective, real-time situational awareness in securing federal information systems. So the long-awaited cybersecurity bill (S. 3480) introduced in the Senate June 10 by Sens. Joe Lieberman (I-Conn.), Susan Collins (R-Maine) and Thomas Carper (D-Del.) is welcome news — and an important milestone that should draw cheers from many quarters.

The 2010 Protecting Cyberspace as a National Asset Act stands out among a recent flurry of congressional efforts to address national cybersecurity, in part for what the bill proposes and what it does not and because of its probability of being enacted.

The legislation, among other measures, would create a White House Office of Cyberspace Policy, led by a Senate-confirmed director, to oversee all federal cybersecurity efforts. It also would create a National Center for Cybersecurity and Communications at the Homeland Security Department to defend .gov networks and oversee the defenses of the nation's most critical infrastructure.

Less visible but equally important, the legislation would set up a more clearly defined framework for government and the private sector to develop a baseline of security requirements that DHS would enforce for that infrastructure. It would provide DHS much-needed help in building its cyber workforce.

The bill also recognizes the role federal procurement can play in getting vendors to do their part in the cyberspace ecosystem by focusing new attention on the potential vulnerabilities in the global supply chain — by requiring language in actual contract specifications, not just the Federal Acquisition Regulation, that addresses the integrity of products delivered to the government.

And it would at last do away with a central flaw of FISMA, by removing the outdated manual reporting requirement that wastes, by some estimates, $500 million every year, and replacing it with a requirement to move toward continuous automated monitoring and a foundation for dynamic cyber defense.

One provision of the bill, not surprisingly, has stirred up vocal concern in industry because it would give the president sweeping authority to order companies to take specific security actions to protect private networks from possible cyberattacks.

The concern is that government is too slow to respond and shouldn't be telling the private sector how to manage its risks. Admittedly, DHS still has a way to go to prove itself. But the bill would actually help DHS better execute its charge to coordinate the situational awareness and forensics activities needed to respond to national cyberattacks. The intent of the legislation is to isolate catastrophic threats. That should actually provide incentives for key industry players to work more closely with DHS for the greater good, which is what this bill is about and why it deserves to reach the president's desk and become law.

About the Author

Wyatt Kash is editor in chief for Government Computer News.