Working Draft (Last edited on 8-20-12; tweaked on 9-7)

U.S. Chamber of Commerce
Analysis of S. 3414, the Cybersecurity Act of 2012

Businesses, Congress, and the Administration Share a Common Starting Point:
The Need for Strong Public-Private Partnerships to Enhance Cybersecurity

Businesses are intently focused on guarding their operations from interruption, preventing the loss of capital and intellectual property, and protecting public safety through employing sound risk-management principles. They devote considerable resources toward maintaining their operations in the wake of a natural hazard or man-made threat, such as a cyberattack. Cybersecurity is viewed as an essential aspect of risk management. Industry activities have included the development of guides and road maps, standards, and innovative technologies to improve security, operational safety, and reliability. Companies routinely strive to strengthen the security of their cyber systems and identify and mitigate any network vulnerability, which requires greater information sharing.

Enhanced cooperation between business owners and operators and government officials is the most effective way to protect critical infrastructures from cyber incidents. Most striking, the federal government and industry are significantly hampered from sharing information by statutes meant for the typewriter age. Legislation is needed to create a sea change in the current information-sharing practices between the public and private sectors while defending personal privacy.

The Chamber continues to urge Congress to pass consensus-oriented cybersecurity legislation—that is, S. 3342, the SECURE IT Act, and H.R. 3523, CISPA—that would actually enhance businesses' efforts to deflect and defeat cyber threats. We agree wholeheartedly with Joint Chiefs Chairman, Gen. Martin Dempsey, who noted recently the crucial importance to both government and industry of swapping information about security risks to computer systems. "I'd like to see a returning Congress push towards cyber legislation that does at least this," the general said. The Chamber supports this view and will continue working toward this end.[1]

Cybersecurity legislation must support public-private partnerships such as the National Infrastructure Protection Plan (NIPP). Businesses work daily to stay a step ahead of nation states (or their proxies), criminal gangs, and rogue individuals to protect sensitive consumer and business information. S. 3414, the Cybersecurity Act of 2012, could do serious damage to working arrangements established by the NIPP, which the Chamber supports. Industry, in partnership with government, has been taking proactive steps for years to guard their information networks and make them more resilient.

The NIPP partnership is being overlooked—if not purposefully sidelined—in the effort to legislate. The NIPP could be undone by Title I (e.g., Sec. 103-104) of S. 3414, which focuses on creating an unproven cybersecurity program that would be multi-sector in scope; dramatically upend existing public-private relationships; or give federal officials too much control over what practices business owners and managers could take to protect their computers and systems.

[1] See "Information Sharing Should Be Key in Cybersecurity Legislation, Joint Chiefs Chairman Says," *CQ Today*, August 14, 2012, available at www.cq.com/doc/news-4141066.

Businesses—either individually or through their sector representatives—need certainty that they would have an equal voice over the design and implementation of a cybersecurity program and that it would be responsive to their needs, effective, and efficient. The bill creates more questions than answers in terms of improving cybersecurity. A new and wholly untested program would likely cause disarray among existing relationships in the NIPP community. These relationships have led to enhancements in sectors' physical and information security, and strong security benefits companies, consumers, and communities.

Included below are just a few of the public-private initiatives under way to guard businesses from theft and disruption. The sampling of initiatives is adapted from NIPP-led sector-specific plans, which can be downloaded at www.dhs.gov/sector-specific-plans.

- **Banking and Finance.** The banking and financial services sector is complex and diverse—ranging from small community banks and credit unions to large institutions. The sector is estimated to have assets of more than $60.8 trillion and accounted for 8.5% of U.S. GDP in 2010. The sector employed 5.8 million workers in 2011. While diverse, a unifying goal of the banking and financial services sector is to maintain its operations in the wake of a natural hazard or man-made threats such as a cyber incident. Industry leaders understand that it is imperative that the sector's information infrastructure be well protected and resilient, enabling customers to entrust their assets to financial institutions and have access to credit. Federal financial regulators have implemented a comprehensive regime that includes the supervision of the banking and financial services sector's operational, financial, and technological systems.

  The current system includes the Federal Financial Institutions Examination Council (FFIEC), whose members conduct regular and continuous examinations to assess the adequacy of institutional controls. These examinations focus on cyber and physical security as well as business continuity, vendor management, and other operational risks as identified in the FFIEC *Information Technology Handbook*. Public sector entities, self-regulatory organizations, and rulemaking bodies provide additional industry oversight to respond to any gaps in cybersecurity practices.

  In addition, working through public-private partnerships, organizations like the Financial Services Sector Coordinating Council and the Financial Services Information Sharing and Analysis Center (FS-ISAC) serve to protect the financial services community against an array of risks. For example, the FS-ISAC acts as a trusted third party, allowing members to submit threat, vulnerability, and incident information in a nonattributable manner so that information can be shared for the benefit of the sector and the nation. The sector also undertakes exercises, which the Chamber has promoted, to assess and improve its own capabilities and often works in partnership with the Treasury Department, federal financial regulators, the Department of Homeland Security (DHS), and law enforcement and national security agencies.

- **Chemical.** The chemical sector is an integral component of the U.S. economy, converting various raw materials into more than 70,000 diverse products, employing nearly 1.3 million people, and earning revenues of roughly $700 billion per year. Industry members are dependent on IT for their communications and operations. The chemical sector has been a leader in developing methods and processes to address safety and manage risk. The sector has long recognized the need to view cybersecurity as an essential aspect of risk management. Industry activities have included development of guides and standards to help improve operational safety and reliability.

  In close partnership with federal officials, the chemical sector has developed a dynamic roadmap (*Roadmap to Secure Control Systems in the Chemical Sector*) describing what is required to improve the cybersecurity of industrial control systems. These control systems were often designed to operate without a connection to a wide area network; they are increasingly becoming linked to corporate or business networks to increase market efficiencies and real-time information flows. However, industry has taken proactive steps to guard its control systems, and the roadmap provides a means of sharing smart and effective measures across the sector. Implementation of the roadmap by the sector is being coordinated by a DHS working group composed of representatives of government and industry. This group also interacts with those working on similar programs in other critical infrastructure sectors.

- **Communications.** The communications industry, an integral part of the U.S. economy, includes wireline, wireless, satellite, cable, and broadcasting providers. Its infrastructure underlies the operations of businesses, public safety organizations, and government. Over the last 25 years, the communications industry has evolved from a predominantly voice-centric service into a diverse, competitive, and interconnected industry that supports the Internet and other key information delivery systems. Commercial carriers devote considerable resources and expertise toward identifying and mitigating threats on the Internet as they are emerging. They take action 24/7, as allowed by law, to address spam, phishing, and other malicious activity that threatens to disrupt their own networks or their customers' use of it.

  Businesses invest heavily in threat detection and mitigation technologies; they also make strategic research and development investments to tackle emerging and future threats. Furthermore, the communications industry works closely with the government on national security and emergency preparedness through partnerships, such as providing the President with policy advice through the National Security Telecommunications Advisory Committee as well as operational support through the National Coordinating Center for Telecommunications (NCC) and the Communications Information Sharing and Analysis Center (C-ISAC). In addition, the Communications Sector Coordinating Council (CSCC), established in 2005, acts as the principal entity for coordinating with the government in implementing national infrastructure protection and response plans.

  The National Cybersecurity and Communications Integration Center (NCCIC) was launched in October 2009. It unites the communications sector coordination of the NCC

and the cyber protection efforts of the United States Computer Emergency Readiness Team (US-CERT). Industry partners are currently testing industry-to-industry information sharing to provide policy recommendations to the President and enhance NCCIC operations.

- **Electric.** The use of electricity in the United States is ubiquitous, spanning all sectors of the economy. More than 70% of electricity customers are served by shareholder-owned electric companies, which are highly regulated. In 2009, electric power accounted for nearly 40% of all energy consumed in the United States. Electric sector owners and operators routinely strive to strengthen the security of their control systems and identify and mitigate any network vulnerability. Protecting the power grid from cyberattacks requires a coordinated effort and the exchange of timely and actionable cyber threat information between industry stakeholders and federal officials.

  To maximize the cybersecurity of the bulk power system, electric utilities work closely with the North American Electric Reliability Corporation (NERC), an industry regulatory body empowered by statute and strictly supervised by the Federal Energy Regulatory Commission (FERC). The mandatory and enforceable critical infrastructure protection (CIP) standards resulting from this established regulatory model already require FERC-regulated utilities to implement numerous countermeasures against potential cyber and physical attacks on critical electric infrastructure. This regulatory regime also facilitates the coordination of cybersecurity protection measures and threat information between utilities, FERC, DHS, and the Department of Energy (DOE).

  Another signature public-private effort includes the development of the Roadmap to Secure Control Systems in the Energy Sector to help focus and make actionable various security initiatives. In addition, the electric industry has contributed to the Smart Grid Cyber Security Strategy and Requirements framework to ensure that cybersecurity protections are incorporated into both the grid's existing architecture and emerging smart grid technologies. A significant variety of industry stakeholders also participate in the development and implementation of the DOE's Electricity Subsector Cybersecurity Risk Management Maturity Model, a tool that allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments. On top of these multi-tiered efforts, most industry members voluntarily participate in the Transmission Forum, which administers numerous audits that focus on security and standards compliance at member utilities, while serving as a valuable information exchange between senior system operators and utility company senior operational executives.

- **Oil and Natural Gas.** The oil and natural gas (ONG) industry features the exploration, production, storage, shipment, and delivery of crude oil and natural gas. Oil and natural gas are imported and produced domestically, stored throughout the United States, and transported over millions of miles via pipelines, waterways, railways, and highways. ONG company owners and operators recognize that their industry has crucial links to other critical infrastructure sectors (and vice versa) and is integral to the nation's energy supply.

Oil and natural gas are vital to the success our nation's economy and energy security. More than 9 million Americans depend on the ONG industry for their jobs. In 2010, the production of oil and natural gas on federal lands brought $9.2 billion into the treasuries of federal and state governments and Indian tribes. Nearly $6.5 billion of that amount came from ONG production. Although the share of non-fossil fuels continues to grow, the ONG industry will continue to play a leading role in meeting U.S. energy needs. Today, oil and natural gas supply more than 60% of the nation's energy demand. According to the U.S. Energy Information Administration (EIA) forecasts, the ONG industry will continue to supply roughly 60% of the nation's energy needs through 2035.

The ONG industry has worked in close partnership with government entities to identify cyber vulnerabilities and develop mitigation strategies. Through extensive coordination and the contribution of technical expertise, the ONG subsector and DOE developed the *Roadmap to Secure Control Systems in the Energy Sector* (2006), which identifies concrete steps to secure control systems in the electric sector and ONG industry.

In addition, collaborative efforts to enhance U.S. cybersecurity are under way with the DHS Industrial Control System Cyber Emergency Response Team related to information sharing and training; with the Transportation Security Administration's (TSA) Transportation Systems Cyber Security Working Group for the development of cybersecurity risk assessment methodology; and with DHS and the Department of Defense to prioritize the security of cyber-dependent business functions. A long list of recommended practices, standards, and guidelines, including the TSA *Pipeline Security Guidelines* (2011), are employed by industry operators to bolster their cybersecurity posture and resilience in an all-hazards context.

National Infrastructure Protection Plan (NIPP) at a Glance

The NIPP provides a unifying framework that integrates a range of efforts designed to enhance the safety and security of our nation's critical infrastructure. The overarching goal of the plan is to build a more safe, secure, and resilient America by preventing, deterring, neutralizing, or mitigating the effects of a terrorist attack, cyber incident, or natural disaster and to strengthen national preparedness, response, and recovery in the event of an emergency.

The NIPP was developed by critical infrastructure partners, including federal, state, and local departments and agencies. First released in 2006, the revised NIPP integrates the concepts of resilience and protection and broadens the focus of NIPP-related programs and activities to an all-hazards environment. The Department of Homeland Security (DHS) oversees NIPP management and implementation in collaboration with other federal entities.

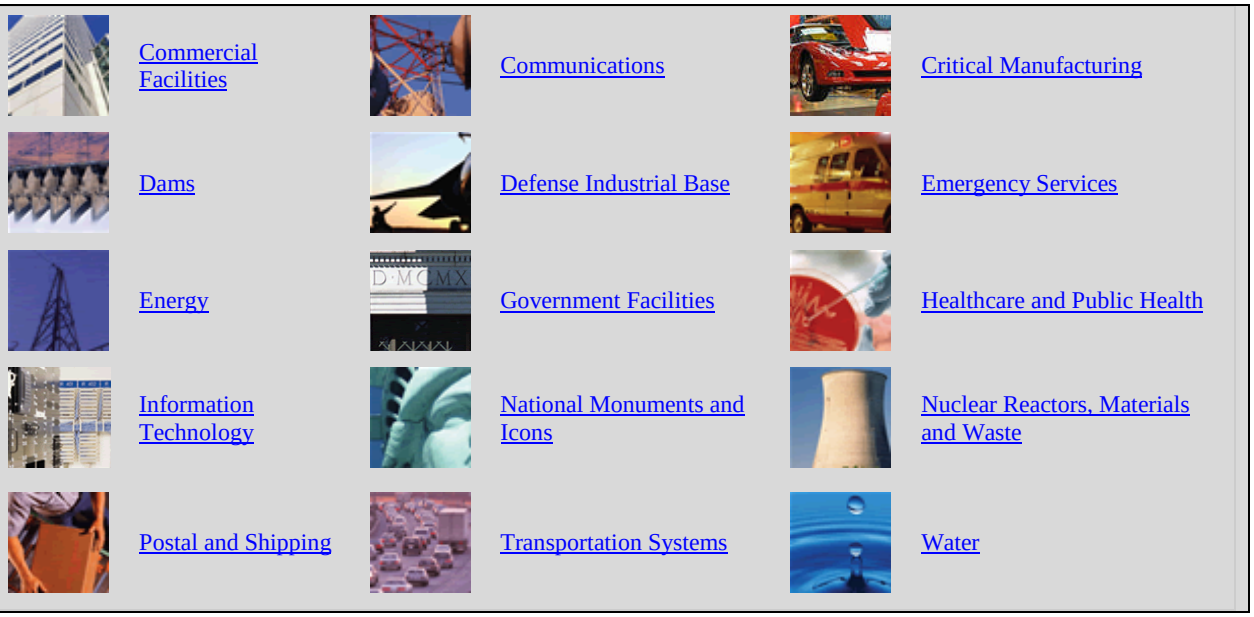
The NIPP assigns a federal agency or department, known as a sector-specific agency (SSA), to lead a collaborative process for critical infrastructure protection within each of the 18 critical infrastructure sectors, which are shown below. Each SSA is responsible for developing and implementing a sector-specific plan (SSP), which details the application of the NIPP framework to the unique characteristics and conditions of its sector.

Critical Infrastructure Sectors


Food and Agriculture


Banking and Finance


Chemical



The business community already complies with multiple information-security rules. Among the regulatory requirements impacting businesses of all sizes are the Chemical Facilities Anti-Terrorism Standards (CFATS), the Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection (FERC-NERC CIP) standards, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley (SOX) Act. The Securities and Exchange Commission (SEC) issued guidance last October that outlines how and when companies should report hacking incidents and cybersecurity risk. Also, corporations comply with many non-U.S. requirements, which only add to myriad regulations.

Instead of adding to the regulatory or quasi-regulatory burden, Congress should work to reduce the fragmented and often conflicting burdens that these different rules and bureaucracies place on industry. Congress, among others, has not adequately acknowledged the contributions that these programs are making to the collective security of the United States. If the Senate had held hearings on S. 3414, it could have learned much about the NIPP framework and the way in which the business community already complies with multiple information-security rules.

It is very disconcerting to see that Congress is prepared to give DHS a dominant role in regulating the cybersecurity of the private sector when the department has not managed the Chemical Facilities Anti-Terrorism Standards (CFATS) program effectively. Sen. Grassley recently said on the floor of the Senate that CFATS was the department's first major regulatory foray, and its management of the chemical security program has been called into question. "The Department of Homeland Security spent nearly a half a million [billion?] dollars on that program. Now, five years later, they've just begun to achieve site security plans for the more than 4,000 facilities designated under the rule." He added that he was "baffled why we

[lawmakers] would take an agency that has proven problems with overseeing a critical infrastructure and give them chief responsibility for our country's cybersecurity."[2]

The Chamber appreciates the work that many senators and staff have put into writing cybersecurity legislation. The Chamber also appreciates the efforts that Sens. Lieberman, Collins, and others have put into crafting a bill to address some of the concerns that have been raised by industry, but fundamental disagreements remain. Our organization's many concerns with the bill are highlighted on the pages that follow. Chamber concerns are manifested, thematically, in at least three points:

- Title I of S. 3414 would give federal officials too much authority over what actions business owners and managers could take to protect their computers and networks. It is unclear that a national cybersecurity program would be managed effectively and nimble enough to respond to quickly changing threats. The existence of a cybersecurity program, linking industry standards to weak liability protections, creates the presumption of an industrywide standard of care.

- Title VII of the bill may actually set back the sharing of information between business and government. The bill's hub-and-spoke model and its strict definition of cyber threat information may erect—not bring down—barriers to productive information sharing. Add to this the problem that liability protections related to voluntary information sharing are vague, if not purposefully qualified, and would invite—rather than deter—lawsuits.

- There are no quick fixes that can achieve what should be a central goal of S. 3414: helping businesses battle sophisticated cyber threats. The bill could actually impede U.S. cybersecurity by shifting businesses' resources away from implementing robust and effective security measures and toward battling red tape.

[* indicates Chamber comment]

Title I Critical Infrastructure

Notable Provision(s) by Section	S. 3414; Senate Amendment (SA) 2731 to S. 3414 (Sec. 103-107) makes 5 changes to the base bill and are indicated below.
National Security Council (Sec. 101)	Establishes a National Cybersecurity Council (Council), which would be composed of government representatives appointed by the President: *** The Council includes no private sector representation. The Council's authority is unbounded and so is the scope of *critical cyber infrastructure* that could be identified or covered.** Council members: DHS secretary (chair); Departments of Commerce, Defense, Justice, the intelligence community, and sector-specific and

[2] See www.cq.com/doc/hsnews-4140580?wr=RDlYTlRja3lSajZveEc0Y0cwd29BQQ; Sen. Grassley's July 30 letter to DHS, which is available at www.grassley.senate.gov/about/upload/homeland-security-oversight-7-30-12-letter-to-Napolitano-about-the-CFATS-program.pdf.

	regulatory agencies. *** The Chamber is concerned about the role, possibly unbridled, of regulatory agencies (e.g., FCC, FERC) vis-à-vis the Council.** *** Council actions could lead to overlapping and conflicting regulations. In some cases, DHS would have the final say in its role as the chair, which would not automatically lead (in our opinion) to positive cybersecurity outcomes. Industry sectors should be aligned with agencies and departments that understand the sectors' histories, requirements, and concerns.**
Inventory of Critical Infrastructure (Sec. 102)	The Council shall designate a federal agency to conduct top-level assessments of cyber risks to critical infrastructure. The input of critical infrastructure (CI) owners and operators, including the Critical Infrastructure Partnership Advisory Council (CIPAC) and information-sharing and analysis organizations, is voluntary. *** "Voluntary" could lead to exclusion. "Voluntary" could also lead to an imbalance in participation and input from small and medium-size businesses. Small businesses, due to fewer resources, could get shut out of the vital decision-making processes and yet would be bound by the criteria of any national cybersecurity program.** The Council shall identify categories of *critical cyber infrastructure* in each sector. The process is to incorporate, to the extent practicable, the input of CI owners and operators. *** Input from sector representatives, as envisioned under the NIPP/CIPAC framework, is nonbinding.** *** The current inventory process is managed by the sector-coordinating councils (private bodies) in collaboration with government partners. The process identifies potentially vulnerable elements of CI.** *** Shifting the identification and prioritization of CI to the Council would marginalize input from the private sector and would run the risk of politicizing the process.** Procedures are to be established that would allow a CI owner to challenge the identification. (The previous bill, S. 2105, has a similar provision pertaining to "covered critical infrastructure.") *Critical cyber infrastructure* (and owners) is identified within each CI sector if damage to or unauthorized access to such CI could result in: --The interruption of life-sustaining services.

	--Catastrophic economic damage to the United States. --Severe degradation of national security. Owners of *critical cyber infrastructure* shall report "significant cyber incidents" affecting *critical cyber infrastructure* (procedures to be created by the Council). *** The burden on owners and operators to report "significant" incident information to federal officials could be quite heavy.** *** The proposal lacks any comparable requirement for DHS or any other government entity to share threat information with CI, which is something industry representatives regularly request.** Limitations: The Council may not identify as *critical cyber infrastructure* IT products and commercial items that organize or communicate information electronically. Congress is provided time (60 days) to review the identification of categories, but the bill is silent on whether lawmakers would be allowed to challenge a designation.
Voluntary Cybersecurity Practices (Sec. 103) (SA 2731 makes 3 changes to Sec. 103)	Within 180 days of enactment, each sector-coordinating council shall propose shall propose "voluntary outcome-based cybersecurity practices"—e.g., industry best practices, standards, and guidelines—to the Council. (Sec. 103(a)) *** More than 180 days will likely be necessary for sectors to execute this portion of the cybersecurity program.** --The cybersecurity practices must be sufficient to remediate or mitigate cyber risks identified in government risk assessments (see Sec. 102). (Sec. 103(a)) *** It is probable that the Council and sectors would disagree periodically on the nature of the "risks" and hence on the appropriateness of certain cybersecurity practices. The bill seems to compel companies to defer to the authority of the Council.** --The Council shall consult with CI owners and operators and other entities (e.g., universities and national labs) to review the cybersecurity practices proposed by the sector-coordinating councils and consider any amendments necessary (in the Council's determination) to address the risks identified in government risk assessments. (Sec. 103(b)) *** This consultation process seems to be occurring at the same time as the sector risk assessments (as called for in Sec. 102). However, sectors should first know the results of the risk assessments before they formulate and recommend cybersecurity practices to the Council.**

	The Council shall adopt any proposed cybersecurity practices that adequately address risks identified in government risk assessments and shall adopt any additional practices that may be necessary (according to the Council's determination). (Sec. 103(b)(2)) *** The Council must not think of itself as a *regulator*, which is the likely practical outcome of S. 3414.** *** Currently, sector-coordinating councils provide input into the National Sector Risk Assessment (NSRA) and develop sector-specific plans to address cyber and physical threats. This effort is done in collaboration with DHS, sector-specific agencies, and its Homeland Infrastructure Threat and Risk Analysis Center (HITRAC).[3] The Council could negatively disrupt a threat identification and mitigation process that is *working*. The Chamber believes that the risk assessments and best practices need to be developed principally by experts in the private sector, with advice from government partners with cybersecurity expertise.** *** The private sector should have meaningful input on what constitutes acceptable cybersecurity practices. Without it, the cybersecurity program would likely become the government-driven, compliance-oriented regime that industry has its voiced skepticism for years.[4]** *** The Council could choose to ignore private-sector input and dictate a "solution" to any given a sector. Industry does not get an equal vote on the Council's approval of the cybersecurity practices.** If a sector-coordinating council fails to propose any cybersecurity practices within 180 days of enactment of the bill, the Council shall decide which practices to adopt. (Sec. 103(b)(2)(B)) The Council and each sector-coordinating council shall assess the cybersecurity practices at least every 3 years. (Sec. 103(c)) Tech Neutrality: No cybersecurity practice shall require the use of a specific Commercial IT product or that it be designed, developed, or manufactured in a particular manner. (Sec. 103(f)) ~~Cybersecurity practices may be adopted as "mandatory requirements" by any federal regulatory agency. If they are not adopted as mandatory requirements, the agency must report to Congress on why they did not do so.~~ (Sec. 103(g)(1)) *** SA 2731 strikes Sec. 103(g)(1) of base bill.**

[3] www.dhs.gov/about-hitrac

[4] See, for example, www.forbes.com/sites/jodywestby/2012/07/27/urgent-businesess-must-act-to-stop-congress-on-cyber-legislation/.

	* **SA 2731 also strikes the "Avoidance of Conflict" Provision, Sec. 103(g)(2), to ensure that "voluntary" cybersecurity practices do not conflict with laws or regulations that CI owners and operators must already comply with.** ~~Where regulations or compulsory standards already exist, the cybersecurity practices shall, to the greatest extent possible, "complement or otherwise improve the regulations."~~ (Sec. 103(g)(3) *** SA 2731 strikes this provision.** Sector-coordinating councils and the CIPAC are authorized to conduct an independent review of the cybersecurity practices. (Sec. 103(h) *** The degree of independence that private entities would have in practice is questionable.**
Voluntary Cybersecurity Program for Critical Infrastructure (Sec. 104)	Within 1 year following enactment, the Council, in consultation with CI owners and operations and the CIPAC, shall establish the Voluntary Cybersecurity Program for Critical Infrastructure ("cybersecurity program" throughout this paper). Any owner of *critical cyber infrastructure* or CI (that is not *critical cyber infrastructure*) may apply for certification under the cyber program. *** The bill makes no attempt to estimate the cost of certification to businesses, which could be prohibitive to small and medium size businesses. (To our knowledge the bill has not been "scored" or priced.)** Owners shall select and implement cybersecurity measures that satisfy the cybersecurity practices established by the Council. *** What's concerning, Council-selected measures could compromise collective security. By homogenizing sectors' standards and practices, the United States' adversaries could quickly learn to circumvent a company's protections and those of similarly situated companies.** Owners must either certify to the Council (under penalty of perjury) that the owner has developed and effectively implemented cybersecurity measures sufficient to satisfy the cybersecurity practices established by the Council or submit an assessment to the Council. The Council may revoke a certification for failing to correct any deficiencies if the Council determines that the owner is not in compliance with the cybersecurity practices.

	Third-party assessments: The Council, in "consultation with" owners and operators and CIPAC, shall enter into agreements with third-party private entities to assess whether a certified owner is complying with "all applicable cybersecurity practices." *** The Chamber is concerned about proposals calling on the owners and operators of *critical cyber infrastructure* to be evaluated by third parties. Complying with third-party assessments would be costly and time consuming, particularly for small businesses.** *** The free market should drive the requirement for third-party certifications, such as with ISO (International Organization for Standardization) certifications. Government should not mandate third-party assessments.** *** Many in the business community are concerned that the release of massive amounts of proprietary information to third parties (and the government) could actually create new security risks.** The Council may perform other assessments if there is a "reasonable suspicion" that an owner is not complying with the cybersecurity practices established by the Council. An owner must provide the Council or a third-party assessor with "any reasonable access" to information necessary to complete an assessment, which is a major concern within the business community given its scope. *** The "reasonableness" language in the above two provisions is problematic. It could open businesses' doors wide open, allowing third parties and the government access to an incredible amount of sensitive information.** *Benefits of certification (incentives):* --Limitations on civil liability. *** Not full protection; only a bar to punitive damages if the certified owner is in substantial compliance with the appropriate cybersecurity practices at the time of the cyber incident.** *** The existence of a cybersecurity program, linking industry standards to liability protections, creates the presumption of an industrywide standard of care. Businesses that do not "voluntarily" opt in could be exposed to legal challenges.** --Expedited security clearances for personnel of certified *critical cyber infrastructure*. *** The government needs to expedite clearances for all applicants, independent of the cybersecurity program. How the government would process a new influx of CI owners and operators is far from clear.**

	--*Critical cyber infrastructure* owners may get prioritized technical assistance. --Provision of cyber threat information. *** This aspect of the bill, which is highly counterproductive, could be construed as withholding from the CI owners and operators cyber threat information if they don't "voluntarily" join the cybersecurity program.** --Public recognition of certified owners of *critical cyber infrastructure*. *** Could lead to attacks on those entities that are perceived to be strong or weak.** Study to examine benefits of procurement preference for certified owners. *** Policymakers should recognize that many procurement preferences already compete with each other in the federal marketplace, so adding another preference could further shrink industry's ability to engage in full and open competition for federal contracts.** Additional comment regarding Sec. 104: *** The Murkowski amendment (SA 2690) to S. 3414 would extend the benefits of the "voluntary" cybersecurity program to entities subject to mandatory requirements (electric and nuclear sectors)**.
Rules of Construction (Sec. 105) (SA 2731 makes 1 change to Sec. 105)	Nothing in this Title shall be construed to-- ~~(1) limit the ability of a Federal agency with responsibilities for regulating the security of critical infrastructure from requiring that the cybersecurity practices developed under section 103 be met~~; . . . *** SA 2731 strikes Sec. 105(1), which stated that nothing in the Title should be construed to limit the ability of a federal agency from requiring that the cybersecurity practices be met.**
Annual Assessment of Cybersecurity (Sec. 107) (SA 2731 makes 1 change to Sec. 107)	Within 1 year of enactment, S. 3414 requires the Council to submit an annual assessment to Congress that includes an analysis of whether the owners of critical cybersecurity practices are "successfully implementing cybersecurity practices." (Sec. 107(b)(2)(B) *** It seems unrealistic that the annual assessment could judge whether U.S. CI is "effectively secured from cybersecurity threats, vulnerabilities, and consequences" when no acceptable, peer-reviewed method exists today to measure aggregate U.S. security. Plus, once the study is completed, many of the threats would have changed, making the study outdated.**

	~~Also included in the assessment is an analysis of whether federal regulatory agencies are "adequately adopting and enforcing" the cybersecurity practices established by the Council.~~ (Sec. 107(b)(2)(C)) *** SA 2731 strikes Sec. 107(b)(2)(C).**
Effect on Other Laws (Sec. 109)	Sec. 109 states, "Except as expressly provided in section 104(c)(1) [civil liability] and section 106 [protection of information], nothing in this Act shall be construed to preempt the applicability of any State law or requirement." *** The federal preemption provisions in S. 3414 are vague, if not simply too weak to act as a meaningful incentive to participate.**

Title II FISMA Reform

Notable Provision(s) by Section	S. 3414, cont.
Sec. 201-204	The bill retains a central role for the secretary of DHS, as opposed to allocating responsibilities among the heads of DHS, OMB, and NIST. (p. 50) S. 3414 authorizes the secretary of DHS to use "protective capabilities . . . for communications or other system traffic transiting to or from or stored on an agency information system without prior consultation," in the event of an "imminent threat." *** This provision could give DHS the authority to exert control over private networks used by the government and any private network that transmits information to or from a federal system, which could entail considerable reach into private networks. (p. 59)** *** The bill consolidates various DHS resources, authorities, and responsibilities within the National Center for Cybersecurity and Communications (Center); the bill expands the role of DHS in information sharing, creating confusion and vagueness with respect to the relationship of this provision to Title VII. The bill appears to give DHS authority to mandate that owners and operators of CI take certain actions related to information sharing, national security, resilience, or emergency preparedness. (Approx. pp. 90-100)** Establishes within DHS a Center, headed by a Senate-confirmed director who reports directly to the Secretary. (pp. 90-91) The budget ("sufficiency of resources plan") for the Center is not required to be provided to OMB and Congress until 120 days after

	enactment. (p. 98) The Center's director shall establish procedures to ensure appropriate sharing of classified cybersecurity information affecting federal or and nonfederal entities, including national information infrastructure (private). (p. 99) Information submitted to the federal government under this subtitle may not be used as evidence in a regulatory enforcement action. *** However, the bill may not bar the information's use more generally for regulatory purposes, which would be a disincentive to share. (p. 101)** The director of the Center shall establish an information-sharing program for federal agencies. (pp. 102+) Additional note: The Chamber has expressed its support for S. 3342, the SECURE IT Act. However, we have noted concerns with Sec. 3554 of Title II of the bill related to FISMA reform and its potential to impact the cyber or IT supply chain. --The Chamber wants to ensure that government entities continue to acquire the most innovative and secure technology products and services under provisions. --Further, federal officials who manage agencies' information security programs should leverage industry-led, globally accepted standards for security assurance during the acquisition process. --Revised language in SECURE IT (S. 3342 compared with S. 2151), stipulating that the bill would not convey any new regulatory authority to agencies or departments, is a step in the right direction. *** The Chamber's concerns related to regulating the <u>IT supply chain</u> extend to any existing bill or proposed legislation.**

Title IV Education, Workforce, and Awareness

Notable Provision(s) by Section	S. 3414, Cont.
Marketplace Information (Sec. 415)	Among other things, Sec. 415(c) states that within 1 year of enactment, the SEC shall evaluate existing guidance to registrants related to disclosures by registrants of information security risks and related events (e.g., SEC Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2, Cybersecurity) to determine whether such guidance should

	be updated by the Division of Corporation Finance or issued as SEC interpretive guidance. *** Sec. 415 appears designed to compel businesses that suffer from a cybersecurity event to publicly disclose the occurrence. This part of S. 3414 aims to name-and-shame companies and could compromise their security.** *** Businesses' sensitive security information should not be disclosed publicly. SEC officials have written to the Senate (June 2011) stating that that investors have not asked for more information on this topic. Further, neither the SEC nor shareholders have the expertise to properly evaluate cybersecurity matters.** *** There is no equivalent disclosure or reporting requirement for government agencies.**

Go to next page.

Information Sharing Legislation—S. 3414 and S. 3342, the SECURE IT Act—Compared

Notable Provision(s)	S. 3414 (Title VII)	SECURE IT (Title I)
Framework for Sharing Information	***Creates a hub-and-spoke system of cybersecurity exchanges, including a designated federal entity acting as the lead exchange (presumably DHS), to protect cyber networks.*** The Secretary of DHS, in consultation with the DNI, Attorney General, and the Secretary of Defense, shall establish a process for designating appropriate civilian government and private-sector entities as cybersecurity exchanges to receive and distribute cybersecurity threat indicators. (Sec. 703) **** S. 3414 suffers from at least 3 fundamental flaws:*** **--It restricts the entities that businesses may share information to those participating in the cybersecurity regime. Information sharing could be greatly diminished for businesses that don't participate or lack a certification. The clear message is: "'Voluntarily' join the cyber program or threat information could be withheld from your enterprise."** **--The bill's strict definition of "cybersecurity threat indicators" would likely create information-sharing silos.** **--The limitation on liability and good-faith defense provisions are arguably so vague and so hedged as to render them meaningless as a genuine incentive for businesses to share information widely.**	***Facilitates the sharing of cyber threat information through existing federal cybersecurity centers.*** Authorizes, notwithstanding any other provision of law, the voluntary sharing of cyber threat information with a cybersecurity center or with any other entity. (Sec. 102(a)) Requires entities providing cybersecurity services to the federal government to disclose any significant cyber incidents to the agency or department that they are protecting. (Sec. 102(b)) The bill contains an "anti-tasking restriction," stating that the federal government cannot do the following: --Require an entity to share information with the federal government except under Sec.102(b) --Condition the sharing of cyber threat information with a business unless the business shares cyber threat information with the federal government. (Sec. 104(b)) *** The framework, which takes a more liberalized approach to information sharing than S. 3414, does not seem to favor one cybersecurity center over another—civilian or noncivilian.**

Liability Protections	No civil or criminal action shall be brought against private entities that voluntarily disclose cybersecurity threat information: --To a cybersecurity exchange. --From a cybersecurity services provider to a customer. --To a private or federal entity that manages CI. --To any other private entity under Sec. 702(a) if the cybersecurity threat information is also disclosed "within a reasonable time" to a cybersecurity exchange. (Sec. 706(a)(2)) If liability protection is not granted, Sec. 706(b) provides for a good-faith defense related to disclosures not protected under Sec. 706(a). *** The liability protections are vague—thus inviting rather than eliminating the very litigation costs and risks that they are supposedly designed to prevent—and throw the effectiveness of this "carrot" into question.** *Additional concerns with the liability protections include:* *** If the bill is enacted, private-sector entities apparently could not share information voluntarily with noncivilian agencies and receive liability protections. Provisions meant to clear up disagreements on this point add to the uncertainty. (See Sec. 703(a)(1), 703(f), 707(a)(4))**[5]	"No cause of action shall lie or be maintained in any court against any private entity" for: --The use of countermeasures. --Any use, receipt, or disclosure of any cyber threat information. --Any actions or inactions in response to the receipt of cyber threat information. (Sec. 102(g)) *** The liability protection provisions in Sec. 102(g) of SECURE IT are clearly stated and leave little or no doubt as to their intent, which is to spur the sharing of cybersecurity threat information between vetted businesses and government entities.** There's no liability for nonparticipation. (Sec. 104(c))

[5] In discussing S. 3414 on the Senate floor, Sen. Franken said, "So I think we negotiated a good series of agreements on this which … will ensure that companies who share cybersecurity information with the government give it directly to civilian agencies and not to military agencies [underlining added]. That was a concern people had." (See July 26, 2012, *Congressional Record*, S5429.)

	*** The bill provides affirmative authority and liability protections related to monitoring activities (see Sec. 701(a)(1) and 706(a)(1)); it does not authorize general liability protection for the use of countermeasures.** *** The bill provides full liability protection only if disclosure of a cybersecurity threat indicator is to an exchange, a customer (if entity is the services provider), a manager of critical infrastructure, or to any other private entity if the indicator is also provided to an exchange. (Section 706(a)(2)(D)) This latter qualification (providing to an exchange) amounts to mandated sharing with the government in order to have full liability protection.** *** Requires "<u>reasonable</u> good faith reliance" that the Title's information-sharing provisions "permitted the conduct complained of is a complete defense" [underlining added]. (Section 706(b)) The ambiguity of private right of action and good-faith provisions is a concern. These cases are likely to be litigated.** *** Failure to disclose threats in a timely fashion is only exempt from liability if the AG or DHS secretary approves of the delay. (Section 706(d))** *** The limitation on liability for "failure to act" does not extend to officers, employees, or agents of a private entity. (Section 706(e))** *** No liability protection for a person who "<u>knowingly</u> or acting in <u>gross negligence</u>" violates a provision of this Title, and such person is subject to criminal action [underlining added].**	

	(Section 706(g)) *** Sec. 706(g) seems to preserve criminal and civil causes of action against private entities under state or federal law that "knowingly or acting in gross negligence" violate this Title or (future) regulations promulgated under the Title.** *** Actions for violations of this Title may be brought in federal or state court, leading to inconsistent rulings and forum shopping to test the exemptions to liability. (Section 706(g))**[6]	
Disclosure Protection (FOIA)	Information exempt from FOIA; treated as voluntarily shared information. (Sec. 704(d))	Disclosures are exempt from FOIA. (Sec. 102(c)(4-5) Information shared with the federal government is proprietary and cannot be shared further without the written consent of the company. (Sec. 102(c))
Regulatory Actions	Cybersecurity threat information shared with the federal government cannot be used "against the entity that lawfully shared the cybersecurity threat indicator" with a federal exchange in a regulatory enforcement action. (Sec. 706(c)) *** Entities that are not the senders of the information are still subject to regulatory actions. And the information must be given to a federal exchange (e.g., DHS), which excludes safeguards if (say) the information is given to a private exchange.**	Cyber threat information cannot be used to regulate the lawful activities of any entity. (Sec. 102(c)(8))
Cybersecurity Threat Information/ Indicators	The original Lieberman-Collins bill from the 112th Congress, S. 2105, permitted private entities to monitor their systems and share information related to "cybersecurity threats," a more general	"Cyber threat information" defined at Sec. 101(4).

[6] Additional commentary on the liability limitations of S. 3414 is available at www.lawfareblog.com/2012/07/the-puzzling-liability-limitations-of-the-lieberman-collins-bill/ and www.lawfareblog.com/2012/07/guessing-what-section-706d-of-the-lieberman-collins-cybersecurity-bill-means/.

	term. However, S. 3414 removes the term "cybersecurity threats" and replaces it with a specific list of cyber threat activities contained in the definition of "cybersecurity threat indicator." (Sec. 701, 708) A cybersecurity exchange may only use, retain, or further disclose cybersecurity threat indicators it receives for two purposes: --To protect information systems from cybersecurity threats. --To provide them to law enforcement for the investigation of a narrow category of crimes (e.g., cyber crime, imminent threat of death, child exploitation). (Sec. 704) *** Under S. 3414, the government is not allowed to use any cybersecurity threat indicator received by an exchange for national security purposes.**	
Antitrust Exemption	No specific antitrust exemption is provided.	Yes. Exempts the sharing of information between 2 or more private entities from antitrust liability. (Sec. 102(e)(4))
Privacy Protections	S. 3414 arguably prioritizes privacy over information sharing, creating an imbalance.[7] The bill, compared with S. 2105, has more restrictions associated with handling information. *** For instance, the Privacy and Civil Liberties Oversight Board must conduct a review that would analyze the practices of private entities that are taking actions under this Title. (Sec. 704)** *** Also, private entities may use or share information only when the purpose is to protect an information system and to assist certain law enforcement**	Compared with the first SECURE IT bill (S. 2151), the second iteration of SECURE IT makes important changes to enhance privacy oversight. *** Tightens the definition of cyber threat information, which is the crux of the Title because it designates what information may be identified, possessed, used, and shared. (Sec. 101)** *** Clarifies that the bill does not provide any authority for the federal government to use or**

[7] See, for example, www.volokh.com/2012/07/23/the-hacker-protection-act-of-2012/.

	investigations. This narrow purpose, which is different from the more general language used in SECURE IT ("sharing of cyber threat information"), is likely to slow or impede the information sharing contemplated by the bill. **Additional note: Senators and staff have indicated that the Administration and privacy groups support S. 3414, especially with respect to Title VII. However, there seems to be a strong consensus among businesses that their concerns with the bill's contents have been granted less weight than those of the Administration or privacy groups.**	**retain cyber threat information, other than as specified in the bill, and that such restrictions are subject to otherwise applicable federal law. (Sec. 102(c))** *** Authorizes the federal government to undertake efforts to limit the impact on privacy of the sharing of cyber threat information. (Sec. 102(d)(C))** *** Clarifies that state, local, and tribal governments are subject to the same restrictions as the federal government in handling information (Sec. 102(e)(3)); clearly defines state, local, and tribal governments. (Sec. 101)** *** Specifies that the report on implementation performed by the heads of agencies containing a cybersecurity center and the Privacy and Civil Liberties Oversight Board will encompass appropriate metrics to determine the impact on privacy and civil liberties and whether there was inappropriate stove piping. (Sec. 105)** *** Authorizes the Council of Inspectors General on Integrity and Efficiency to review whether the federal government has properly handled cyber threat information. (Sec. 106)**[8]
Federal Preemption	Sec. 707(b) states, "This title supersedes any law or requirement of a State or political subdivision of a State that restricts or otherwise expressly regulates the provision of cybersecurity services or the acquisition, interception, retention, use or	Sec. 102(f) "supersedes any statute or other law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this section."

[8] For more on privacy protections and other topics, see http://thf_media.s3.amazonaws.com/2012/pdf/fs110.pdf.

	disclosure of communications, records, or other information by private entities to the extent such law contains requirements inconsistent with this title." However, Sec. 707(c) states, "Preservation of Other State Law—Except as expressly provided, nothing in this title shall be construed to preempt the applicability of any other State law or requirement." *** The federal preemption provisions in S. 3414 are vague, if not simply too weak to be meaningful.**	*** Federal preemption language in SECURE IT is clearer and stronger by comparison.**