Examples of Support for Public-Private Collaboration	
Global conglomerate, Fortune 100	"We welcome the opportunity to partner with the federal government to help identify our country's cyber vulnerabilities, and jointly develop protective measures that will promote the safeguarding of information critical to national security."
Healthcare, Fortune 100	"Vast federal resources are devoted to cybersecurity, but the current efforts are fragmented. We recommend the establishment of a public-private collaborative effort on cybersecurity that will combine existing federal requirements under a single coordinated framework. This approach will minimize undue complexity and promote a more agile and effective national cybersecurity response."
Communications, Fortune 100	The company "supports the joint development of cybersecurity practices in a collaborative partnership between the public and private sectors…A voluntary program is flexible and adaptable, which is important given the difficulty of predicting cyber-attacks and the speed with which providers must be able to adapt their approach to meet new threats…There are various aspects of the Cybersecurity Act of 2012, however, that conflict with this approach as a practical matter."
Financial Services, Fortune 100	"We support a voluntary program that enables the federal government and the private sector, in coordination, to develop best practices for companies to adopt as they so choose. Such a program would foster open communication and enable companies to make security decisions informed by the best information from the federal government as well as their own experience."
Technology, Fortune 100	The company "urges Congress to continue working to pass cybersecurity legislation that will advance risk management practices, strengthen the protection of critical cyber infrastructure, and enhance appropriate information sharing of actionable information concerning cyber-threats."
Financial Services, Fortune 100	"Additionally, we see the benefit of federal government and private sector collaboration on standards and good practices as the starting point for successful operations and defense against evolving threats. However, we are concerned with the potential duplication of efforts and a lock-step, uniform approach to cybersecurity practices, which would be more vulnerable by not affording resiliency or providing a needed diversity in our defenses to combat the dynamic threat."

Technology, Fortune 100	The company "supports the development of cybersecurity best practices for voluntary adoption and use at critical assets. [The company] believes these best practices should be risk based, focused on secure outcomes, and developed jointly between the government and the private sector. These best practices should also take into account the existing body of cybersecurity industry standards and best practices."
Healthcare, Fortune 100	"The Federal Government can and should provide more detailed and consistent protective advice to private industry, perhaps through the Critical Infrastructure Partnership Advisory Council…The federal government has a unique perspective in determining the elements of critical infrastructure in the United States. This step, taken in coordination with the private sector, could focus appropriate attention on the elements most deserving of increased protection. A 'critical infrastructure' designation should not be applied by sector or by Company, but instead applied more selectively. Such flexibility would allow companies to focus resources on protecting the most important elements of infrastructure. For example, infrastructure that generates electric power is critical, but the billing system for power consumed is not as critical."
Global conglomerate, Fortune 100	"We appreciate your leadership and persistence on this critical issue, and share the sense of urgency most recently expressed by Secretary Panetta on the need to take action to protect the nation's economic and national security against cyber attacks."
Communications, Fortune 100	"A truly voluntary program designed to enable the federal government and the private sector to develop best cybersecurity practices for companies to adopt as they so choose would be a powerful tool in the fight against cyber threats."
Retail, Fortune 100	"We respect and applaud efforts like yours to improve cybersecurity, particularly for critical infrastructure sectors. We agree that protecting America's national security from cyber attacks should be a top priority, and is essential to economic growth and commercial activities of the United States."
Technology, Fortune 100	"Because of the priority we place on security, we support many of the goals of the Cybersecurity Act of 2012, as we believe that both the federal government and the private sector share the same desire of ensuring that our country's truly critical cyber infrastructure are protected and secure…we believe the government should avoid mandatory technology or standards."
Fortune 100	"In general, the company is not opposed to a truly voluntary program whereby those companies

	within the private sector that maintain 'critical infrastructure' develop, in consultation with the federal government, best practices that such companies may follow if they so choose."
Oil & Gas, Fortune 100	"TSA [Transportation Security Administration] standards have been an asset to our company as we continue to build upon and enhance our existing cybersecurity protections. Particularly given the importance of our domestic energy infrastructure, we believe that the development of voluntary standards from the TSA, and more broadly, from the Department of Homeland Security, is a benefit to the industry and we welcome additional opportunities to collaborate with federal agencies. In our view, this type of collaboration between the public and private sector is essential to our nation's efforts to prepare and respond to sophisticated cyber attacks. To this end, we express our support to you for federal legislation that enhances information-sharing and facilitates further cooperation between the private sector and government agencies."
Communications, Fortune 100	The company expresses its "deep appreciation for your tireless efforts to craft legislation that improves the security of our Nation's critical infrastructure."
Chemicals, Fortune 500	"The Federal Government should improve the collaboration across the myriad agencies that play a role in national cybersecurity and with key segments of the private sector. In addition, the private sector should be an active partner in the development and appropriate implementation of industry best practices."
Healthcare, Fortune 100	"In general, we have no problem with the development of voluntary standards which give companies like ours the flexibility to opt-out of these standards if they are deemed too prohibitive from a cost or usability perspective or if they conflict with other obligations to which we are bound."
Financial Services, Fortune 100	"We welcome all activities to develop cybersecurity practices that may inform any necessary risk based improvements in our environment. We continue to support all appropriate efforts through our Sector Specific Agency, in the context of our existing regulatory frameworks. In fact, we are involved in many existing public/private partnerships to continue to develop cybersecurity practices."
Communications, Fortune 500	"We have no concerns with the federal government and private industry collaborating to build cyber security standards if it is voluntary."
Technology, Fortune	The company "supports the development of effective voluntary programs and frameworks that will

500	help strengthen critical infrastructure security. Further, we believe that the inclusion of incentives such as liability protection, are vitally important to the success of such programs."
Transportation, Fortune 500	The company "supports federal efforts to develop, in coordination with the private sector, best cybersecurity practices for companies to adopt as they so choose. We believe a voluntary, coordinated and collaborative process in which the federal government and the private sector work together to develop best practices will go a long way to create a greater level of harmonization and consistency among cybersecurity providers."
Energy, Fortune 500	The company "supports enhancing current public/private partnerships that encourage information sharing as outlined in the Cyber Security Act of 2012." The company "also support[s] other voluntary aspects of the bill as long as they do not create another mandatory regime without consideration of the existing regulatory frameworks overseen by the Federal Energy Regulatory Commission and the Nuclear Regulatory Commission. While [the company] [is] not opposed to a coordinated effort between the federal government and private sector to identify critical cyber infrastructure, any such effort should build on the foundation of work already completed by industry in partnership with FERC/NERC and the NRC."
Energy, Fortune 500	The company "believes the Cyber Security Act of 2012 is a good starting point to facilitate a discussion on the issue of cyber security, and agrees there is a need for additional training dollars to support the next generation of cyber security professionals."
Energy, Fortune 500	The company was "hopeful Congress could reach agreement on legislation to encourage appropriate coordination between the federal government and private sector and in so doing improve the nation's ability to prepare for and defend against cyber threats." The company is "committed to working directly with government partners to more thoroughly understand cyber threats and defend against them. An innovative and cooperative approach between the private sector and federal government is imperative…" "Regarding legislation, the idea of a voluntary program that encourages collaboration between the government and the private sector to develop 'dynamic and adaptable voluntary cyber security practices' does make sense. [The company] believe[s] that any new legislation in this area should focus on information-sharing, should be adaptable and flexible given the changing nature of the threat, and, most importantly, should not seek to supplant the existing regulatory structures and public-private coordination already taking

	place in our electric and nuclear power sectors."
Energy, Fortune 500	"With regard to legislation, [the company] would be supportive of a voluntary program that encourages collaboration between the government and the private sector to develop dynamic and adaptable voluntary cybersecurity practices." The company "believe[s] the program, at its foundation, should be of an information-sharing construct that is nimble enough to address ever-changing threats; should supplement, and not replace, existing public-private partnerships; should be comprehensive across a wide array of interdependent industries; and, should be tasked to a single agency to coordinate its implementation."
Technology, Fortune 500	The company "agrees that cybersecurity best practices should be developed via a partnership between government and industry." The company "supports the creation of a voluntary program based on the DIB model. One key concern is ensuring that company proprietary information being shared with the federal government and potentially other third parties is adequately protected. Unauthorized disclosure of proprietary information could have serious ramifications, including irreparable financial and reputational damage." The company "believes that the secure bilateral sharing of relevant material is fundamental to ensuring that our national security and economic security interests are protected."
Energy, Fortune 500	The company "supports federal legislation that will promote the development of effective cybersecurity practices." The company "continues to believe that it is important that Congress and the federal agencies continue working with the private sector to address these national security issues in a joint and comprehensive fashion that strengthens public-private partnerships, clarifies federal authority, limits duplicative regulatory frameworks and increases the ability to defend our nation's critical infrastructure and train our workforce to counter advanced cyber threats."
Fortune 500	The company has "no fundamental concerns with a voluntary U.S. program if it is indeed voluntary, as opposed to a program developed from a regulatory or compliance perspective or by the unfortunate notion that companies should be required to disclose breaches or vulnerabilities."
Energy, Fortune 500	The company "commend[s] your continued focus on this concern, and share[s] your conviction that a strong, collaborative approach between the private sector and government is essential in helping protect our nation from a sophisticated cyber threat." The company "supports a voluntary program that promotes federal government and private sector coordination regarding cybersecurity

	practices."
Hospitality, Fortune 500	The company "would not be opposed to the development of a truly voluntary set of best practices in cybersecurity among those who maintain critical infrastructure. Similarly, [the company is] in favor of increased cyber intelligence sharing facilitated by enhanced cooperation between the government and the private sector."
Transportation, Fortune 500	The company "is generally supportive of joint private sector/public sector partnerships to explore best practices."
Financial, Fortune 500	The company is "very much in favor of coordination between the federal and private sector with regards to the development of best practices regarding cybersecurity." However, the company is "concerned that the creation of cybersecurity standards that are in addition to and separate and apart from the existing regulatory requirements, supervisory activities and public-private sector information sharing bodies as this may create confusion and divert resources away from addressing cyber threats specific to the financial sector and [their] institution." The company "feel[s] that more information sharing and industry specific standards and oversight based on risk is key to effectively and efficiently countering rapidly evolving cyber threats."

Examples of Support for Information Sharing	
Healthcare, Fortune 100	"We recommend that the government accelerate our nation's cybersecurity preparedness through the promotion of public-private partnerships that will facilitate exchange of strategic threat assessments and other pertinent intelligence . . . This will enable private sector entities that own or operate major information systems and other critical infrastructure systems to respond to emerging cybersecurity threats on a timely basis."
Defense, Fortune 100	"We strongly support efforts to clarify authorities allowing for better information sharing among industry, and between industry and the U.S. Government, specifically with regard to sharing classified signatures."
Pharmaceutical, Fortune 500	"We do believe that additional government initiative would be welcomed that drives more explicit and transparent exchange of threat intelligence between the federal government and the private sector so that we can operate from similar bases of knowledge."
Energy, Fortune 500	"We greatly value the government's role in providing current data about cybersecurity threats . . . We believe that this approach is well suited to the needs of private industry, and results in swift and effective cybersecurity measures."
Energy, Fortune 500	The company "share[s] your goal of protecting the nation's critical infrastructure from cyber threats and encourage Congress to act on legislation which will improve information-sharing capabilities among government and industry." The company "hopes that Congress is successful in passing legislation that will facilitate greater access to security clearances for the private sector and addresses current barriers to information sharing, such as the lack of indemnity protection. Fluid information sharing between critical infrastructure sectors and federal agencies is paramount in defending against cybersecurity threats."
Marketing, Fortune 500	"The development of a truly voluntary program that encourages and facilitates the mutual sharing of important information between the public and private sectors on cybersecurity issues is an important and laudable goal. We believe that any such program, whether legislatively established or otherwise, should be informed by the following principles: No additional regulatory burden … Truly mutual and voluntary information sharing … Regard for individual circumstances … Respect for privacy and data protection."

Example Statements on the Current Role of the Federal Government	
Financial Services, Fortune 100	"Our practices are reviewed on a continuous basis by the Office of the Comptroller of the Currency and the Federal Reserve Bank. In addition, our cybersecurity personnel maintain close contact with local, state and federal law enforcement agencies and are actively engaged in leadership positions of the FS-ISAC, FSSCC and FBIIC. We frequently share information on cyber security trends with various federal intelligence agencies through these well established channels. Specific cyber security cases are worked jointly with the appropriate federal agencies. Our dependency on the sharing of information with these federal agencies has grown in light of recent events . . ."
Financial Services, Fortune 100	"We continue our close partnership with the Federal Government at multiple levels through a vibrant public/private partnership with our Sector Specific Agency (U.S. Department of the Treasury), our Federal Regulators, the Department of Homeland Security, and other parts of Government . . . We are cognizant of the large efforts of the Federal Government in funding research and development, and enabling organizations such as NIST to provide and promote standards for risk based adaptation into our cyber-security practices."
Healthcare, Fortune 100	"The role of the federal government has been significant in the development of…cybersecurity practices in myriad ways."
Energy, Fortune 500	"We use information available from the Department of Homeland Security and other government agencies to understand threats and remediation."
Energy, Fortune 500	"The federal government has played an important role in [the company's] development and adoption of cybersecurity practices and programs."
Financial Services, Fortune 500	"Government has been and must continue to be a critical partner and [the company] is committed to working closely with government agencies to expand and deepen that relationship."

Example Concerns Regarding Mandatory Standards	
Energy, Fortune 100	The company "is concerned that 'voluntary' will lead to 'regulated' resulting in precious resources being diverted away from active threat management to compliance-based activities."
Communications, Fortune 100	"[T]he structure of the proposed NCC [National Coordinating Center,] including multiple government agencies and the unilateral ability for the new entity to trigger audits, is ripe for politicization. In the end, private sector entities . . . would have little choice but to adopt those standards regardless of their cost, effectiveness or effect on their ability to innovate, ultimately making this structure only nominally 'voluntary.'"
Financial Services, Fortune 100	"We have concerns about a program that creates mandatory cybersecurity practices that, while appropriate for some industries, would not be suitable for our industry, with its high concentration of critical infrastructure, significant differences among firms regarding size and risk profile, and extraordinarily sophisticated and well resourced cybersecurity practices."
Pharmaceutical, Fortune 100	"Best practices for cybersecurity are not universally appropriate for all companies. A practice necessary in one setting may be inappropriately restrictive in another. Information security best practices are well documented and understood. A key concern would be the establishment of practices which do not apply to certain industries or types of infrastructure within those industries, especially to the extent that those practices become mandatory in the future."
Fortune 100	The company "has concerns with the Senate's comprehensive cyber security bill due to its industry practices mandates. We have concerns that these would not be flexible enough to keep up with rapidly changing technology and cyber-based threats and could distract companies and government focus on current threat mitigation and information sharing. We believe that a flexible integrated approach to physical, transportation and cyber security that is risked-based/performance-based best serves our company and our industry."

Example Concerns Regarding the "Impact on Innovation"	
Communications, Fortune 100	"We commend your efforts to create legislation designed to improve the security of our nation . . . with the *caveat* that we believe the primary focus on best practices in Title I of the Cybersecurity Act of 2012 is not as optimal for our nation's cybersecurity as promoting and facilitating a primary role for continuous *innovation* in solving our national cybersecurity challenge." "Our concern is that federal legislation not tip the balance in a way that overlooks the complex and interdependent nature of the internet ecosystem as a whole and which results in the imposition of predictability on one or more industry sectors rather than encouraging innovation in all sectors through voluntary collaborations."
Communications, Fortune 100	"We are . . . concerned that shifting the focus to compliance with government standards could deter private sector innovation . . . Rather than direct companies to meet a static set of standards that may become quickly outdated, we think the government should encourage companies to invest and innovate in this area so that a diverse range of solutions can develop that reflect the diversity of network and business environments in the marketplace today."
Technology, Fortune 500	The company "urges the U.S. Government to use open, non-proprietary standards and technology neutral approaches to IT security that enhance competition and innovation while reducing the risk of vendor 'lock-in' and limiting choice and innovation."
Communications, Fortune 500	"Cybersecurity proposals must be technology neutral, flexible enough to promote technological innovation, and global in nature to reflect today's borderless and interconnected cyber environment."

Example Concerns Regarding Duplication/"One-Size-Fits-All"	
Energy, Fortune 500	"A government-led effort will necessarily involve a certain level of 'one-size-fits-all' standardization, which will not only fail to address the specifics of individual company/industry systems and processes, but will also provide a potential 'roadmap' to those who seek to exploit those systems."
Technology, Fortune 100	The company "believes that a successful program must . . . Adopt an outcomes-based approach with clear expectations for 'what' is expected of an organization and not 'how' the organization should achieve it. 'One size fits all,' legislatively-mandated requirements, which are subsequently interpreted narrowly and incorporated into agency regulations, may be too specific and inappropriate for individual company risk environments. Maintaining a flexible approach will ensure that, as technology and threats change, organizations can evolve to best address cybersecurity risks for their particular organization."
Technology, Fortune 100	"Most problematic, in our view, is the very real risk that a static, 'check-the-box' compliance regime will encourage some firms to invest only in meeting static standards or best practices that are outmoded before they can even be published . . . One of the reasons [the company] did not support the Cybersecurity Act of 2012 when it was being considered by the Senate this summer was that we believed the legislation would have led precisely to this kind of top-down, 'check-the-box' compliance regime."
Communications, Fortune 100	"One size most certainly does not fit all in the battle to ensure cybersecurity. Cyber thieves and hackers are innovating on a daily basis, and we must have a policy framework founded on flexibility – rather than prescriptive rules or enforceable performance requirements – so that we can avail ourselves of the growing array of technologies, solutions, and counter-measures that are available to us."
Technology, Fortune 100	"One concern we have with [the voluntary programs described in Sec. 103 and 104] is the extent to which they might be duplicative of existing public-private partnerships such as those under the NIPP . . . the private sector is already empowered to develop such cybersecurity practices through existing public-private partnership (PPP) mechanisms such as the NIPP. It is not clear

	to us whether the proposed programs would be complementary to existing PPPs, or negatively disrupt current threat identification and mitigation processes that are working under existing PPPs."
Energy, Fortune 500	"The challenge created by the Cybersecurity Act of 2012 is establishment of a duplicative layer of standards – however voluntary they may be in the beginning – that will eliminate the electric industry's ability to respond quickly to cyber threats to the nation's critical infrastructure. While there is a role for the federal government to play in this crucial issue, additional standards do not properly fill that role."

Example Concerns Regarding Liability	
Financial Services, Fortune 100	"Although voluntary, we are concerned that the process could ultimately lead to civil lawsuits against a company to the extent the company is not certified under the statute and a plaintiff is seeking a cause of action against a company for cybersecurity-related concerns."
Fortune 100	The company "has concerns that some of the risk assessment requirements would increase the risk of liability and punitive damages. These concerns have been communicated in detail through various industry groups such as The Business Roundtable, American Chemistry Council, and the U.S. Chamber of Commerce."
Technology, Fortune 100	"While much-needed liability protection is offered as another benefit of certification, the proposed CSA12 protection is quite limited, serving as a weak incentive."

Other Concerns	
Energy, Fortune 500	"We are also concerned about regulatory over-reach, in which virtually all systems and facilities will ultimately be designated as critical infrastructure, regardless of their actual threat profile."
Fortune 100	"We are concerned that the appearance of working closely with DHS, law enforcement, or the intelligence community could hinder our ability to compete in non-US markets . . . It is not difficult to imagine a foreign country distancing itself from US companies that voluntarily collaborate closely with its home country's security and intelligence organizations."