Bill Summary & Status
112th Congress (2011 - 2012)
S.3414
CRS Summary

S.3414
Latest Title: CSA2012
Sponsor: Sen Lieberman, Joseph I. [CT] (introduced 7/19/2012) Cosponsors (4)
Related Bills: S.2102, S.2105
Latest Major Action: 11/14/2012 Senate floor actions. Status: Upon reconsideration, cloture on the bill not invoked in Senate by Yea-Nay Vote. 51 - 47. Record Vote Number: 202.

SUMMARY AS OF:
7/19/2012--Introduced.

Cybersecurity Act of 2012 or the CSA2012 - Establishes a National Cybersecurity Council, to be chaired by the Secretary of Homeland Security (DHS) (the Secretary), to: (1) conduct sector-by-sector risk assessments; (2) identify categories of critical cyber infrastructure (CCI categories); (3) coordinate the adoption of private-sector recommended voluntary outcome-based cybersecurity practices; (4) establish an incentives-based voluntary cybersecurity program for critical infrastructure to encourage owners of critical infrastructure to adopt such practices; (5) develop procedures to inform critical infrastructure owners and operators of cyber threats, vulnerabilities, and consequences; and (6) provide any technical guidance or assistance requested by owners and operators.

Directs the Council to designate an agency to: (1) conduct top-level cybersecurity assessments of cyber risks to critical infrastructure with voluntary participation from private sector entities; and (2) prioritize ongoing, sector-by-sector assessments beginning with sectors posing the greatest immediate risk.

Requires the Council to submit each risk assessment to the President and appropriate federal agencies and congressional committees.

Directs the Council to: (1) identify CCI categories within each sector of critical infrastructure and critical infrastructure owners within each category, and (2) establish a procedure for owners of critical cyber infrastructure to challenge the identification.

Directs the Council to identify CCI categories as a critical cyber infrastructures only if damage or unauthorized access could reasonably result in: (1) the interruption of life-sustaining services (including energy, water, transportation, emergency services, or food) sufficient to cause a mass casualty event or mass evacuations; (2) catastrophic economic damage to the United States, including financial markets, transportation systems, or other systemic, long-term damage; or (3) severe degradation of national security.

Requires the Council to establish procedures under which owners of critical cyber infrastructure shall report significant cyber incidents affecting critical cyber infrastructure.

Provides for congressional review of critical cyber infrastructure determinations.

Requires private sector coordinating councils (PSCC) within critical infrastructure sectors established by the National Infrastructure Protection Plan to propose cybersecurity practices to the Council. Directs the Council to adopt: (1) any proposed practices and any necessary amended or additional practices that adequately address identified cyber risks, and (2) practices pursuant to the Council's own assessment if a PSCC fails to submit proposals.

Permits federal agencies with responsibilities for regulating the security of critical infrastructure to adopt such practices as mandatory requirements. Requires agencies that do not adopt the practices to report to Congress on the agency's reasoning, including a description of whether the agency is maintaining practices sufficient to effectively address cyber risks.

Directs the Council to establish the Voluntary Cybersecurity Program for Critical Infrastructure under which owners of critical infrastructure certified to participate in the Program select and implement cybersecurity measures of their choosing that satisfy such cybersecurity practices in exchange for: (1) liability protection from punitive damages; (2) expedited security clearances; and (3) prioritized technical assistance, real-time cyber threat information, and public recognition.

Prohibits any of the above provisions relating to the critical infrastructure public-private partnership from limiting the ability of a federal agency with responsibilities for regulating the security of critical infrastructure from requiring that the cybersecurity practices adopted by the Council be met.

Directs the Secretary to establish a Critical Infrastructure Cyber Security Tip Line.

Requires the Secretary to: (1) inform the owner or operator of information infrastructure located outside the United States the disruption of which could result in catastrophic damage within the United States and the government of the country in which the information infrastructure is located of any cyber risks to such information infrastructure; and (2) coordinate with such governments and owners or operators regarding the implementation of measures to mitigate or remediate cyber risks.

Amends the Federal Information Security Management Act of 2002 (FISMA) to direct the Secretary to oversee the information security requirements of federal agencies. (Currently, the Director of the Office of Management and Budget [OMB] has such oversight authority and has administratively transferred certain responsibilities to DHS through an OMB memorandum.) Revises information security requirements for federal agencies and provides for continuous monitoring and streamlined reporting of cybersecurity risks.

Maintains: (1) the President's oversight over national security systems; and (2) the delegation of authority to the Department of Defense (DOD), Central Intelligence Agency (CIA), and Director of National Intelligence (DNI) for specified defense and intelligence systems.

Amends the Homeland Security Act of 2002 to consolidate existing DHS resources for cybersecurity within a National Center for Cybersecurity and Communications. Sets forth the duties of the Center, including managing efforts to secure, protect, and ensure the resiliency of the federal information infrastructure, supporting private sector efforts to protect such infrastructure, prioritizing efforts to address the most significant risks to the information infrastructure, and ensuring privacy protections.

Requires the Center to be headed by a Director (appointed by the President with Senate confirmation) who reports to the Secretary. Directs the DNI to identify a Deputy Director with concurrence of the Secretary.

Directs the Center to: (1) oversee the national security and emergency preparedness communications infrastructure, including the Office of Emergency Communications and the National Communications System; (2) develop a national incident response plan detailing the roles of federal agencies, state and local governments, and the private sector; and (3) consult with international partners.

Requires the Center to establish procedures to: (1) ensure regular and timely sharing of cybersecurity information between and among federal and nonfederal entities, including cybersecurity centers, network and security operations centers, cybersecurity exchanges, and nonfederal entities responsible for such systems; and (2) share cybersecurity threat and vulnerability information by the federal government with owners and operators of the national information infrastructure.

Prohibits federal entities from: (1) using certain voluntarily submitted information as evidence in regulatory enforcement actions; or (2) unless otherwise authorized by law, compelling a disclosure of information from a private entity or intercepting wire, oral, or electronic communications.

Requires federal agencies, unless otherwise directed by the President, to immediately notify the Center of any incident affecting a national security system.

Directs the Director of the Office of Science and Technology Policy to develop a national cybersecurity research and development plan to encourage the development of computer technologies and software to protect against evolving cyberthreats.

Requires the National Science Foundation (NSF), Secretary, and Secretary of Commerce to establish a program for federal agencies to award grants to institutions of higher education or research and development nonprofit institutions to establish cybersecurity test beds capable of realistic modeling of real-time cyber attacks and defenses.

Directs the NSF to establish cybersecurity research centers based at institutions of higher education and other entities.

Requires the DHS and DOD to jointly establish academic and professional Centers of Excellence to protect critical infrastructure in conjunction with international academic and professional partners from countries that may include appropriate U.S. allies.

Directs the NSF to establish a Federal Cyber Scholarship-for-Service program.

Directs the Secretary to develop and update periodically an acquisition risk management strategy including procedures to: (1) assess risks to the federal information infrastructure supply chain, (2) incorporate internationally recognized standards with input from the private sector, and (3) share threat information with the private sector.

Amends federal information technology procurement laws to provide information security training to contracting officers and promote the acquisition of information security products through authorized channels or distributors of a supplier.

Sets forth the responsibilities of the Department of State with respect to the coordination of international norms for cyberspace to be developed with other countries and the consideration of cybercrime in foreign policy and foreign assistance programs.

Authorizes private entities to monitor and operate countermeasures to protect against cybersecurity threats on their own information systems and the information systems of a third party with such party's express prior consent.

Permits private entities to disclose lawfully obtained cybersecurity threat indicators to other private entities for the sole purpose of protecting information systems. Sets forth requirements for safeguarding information that could be used to identify specific persons and prohibits the use of such information to gain an unfair competitive advantage.

Directs the Secretary to establish a process for: (1) designating one or more civilian federal entities, private entities, or nonfederal government entities to serve as cybersecurity exchanges; and (2) sharing classified and unclassified cybersecurity threat indicators in as close to real time as possible with appropriate entities.

Requires the Secretary to designate a civilian federal entity as the lead cybersecurity exchange for information sharing among federal entities and with state, local, tribal, and territorial governments, international partners, and private entities.

Authorizes federal entities to disclose cybersecurity threat indicators to law enforcement if: (1) disclosure is permitted under procedures developed by the Secretary and approved by the Attorney General (DOJ) to protect privacy and civil liberties; and (2) the information pertains to a cybersecurity crime, an imminent threat of death or serious bodily harm, or a serious threat to minors, including sexual exploitation and threats to physical safety.

Allows law enforcement to use such indicators only to: (1) protect information systems from a cybersecurity threat or investigate, prosecute, or disrupt a cybersecurity crime; or (2) protect individuals from imminent threats of death or serious bodily harm and minors from serious threats.

Defines a "cybersecurity crime" as violation of a state or federal law relating to computer crimes, including any provision of the federal criminal code enacted or amended by the Computer Fraud and Abuse Act of 1986.

Directs federal entities to develop and enforce appropriate sanctions for employees who conduct cybersecurity information activities outside the normal course of duties or in a manner inconsistent with their responsibilities or in contravention of procedures to protect privacy and civil liberties.

Establishes a cause of action against the United States if a federal entity intentionally or willfully violates cybersecurity information laws or related regulations.

Requires the DNI to issue guidelines for granting security clearances. Sets forth standards for sharing classified threat indicators.

Provides legal protections to entities engaged in authorized cybersecurity activities.