HR 3674

PRECISE Act of 2012

Congress: 112 (2011–2013, Ended)
Chamber: House
Policy Area: Emergency Management
Introduced: Dec 15, 2011
Current Status: Placed on the Union Calendar, Calendar No. 501.
Latest Action: Placed on the Union Calendar, Calendar No. 501. (Sep 21, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/house-bill/3674

Sponsor

Name: Rep. Lungren, Daniel E. [R-CA-3]
Party: Republican • **State:** CA • **Chamber:** House

Cosponsors (11 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Bilirakis, Gus M. [R-FL-9]	R · FL		Dec 15, 2011
Rep. King, Peter T. [R-NY-3]	R · NY		Dec 15, 2011
Rep. Langevin, James R. [D-RI-2]	D · RI		Dec 15, 2011
Rep. Long, Billy [R-MO-7]	R · MO		Dec 15, 2011
Rep. Marino, Tom [R-PA-10]	R · PA		Dec 15, 2011
Rep. McCaul, Michael T. [R-TX-10]	R · TX		Dec 15, 2011
Rep. Miller, Candice S. [R-MI-10]	R · MI		Dec 15, 2011
Rep. Stivers, Steve [R-OH-15]	R · OH		Dec 15, 2011
Rep. Turner, Robert L. [R-NY-9]	R · NY		Dec 15, 2011
Rep. Walberg, Tim [R-MI-7]	R · MI		Dec 15, 2011
Rep. Meehan, Patrick [R-PA-7]	R · PA		Feb 16, 2012

Committee Activity

Committee	Chamber	Activity	Date
Energy and Commerce Committee	House	Discharged From	Sep 21, 2012
Homeland Security Committee	House	Reported by	Feb 1, 2012
Intelligence (Permanent Select) Committee	House	Discharged From	Jul 11, 2012
Judiciary Committee	House	Referred to	Jan 6, 2012
Oversight and Government Reform Committee	House	Discharged From	Jul 11, 2012
Science, Space, and Technology Committee	House	Referred to	Jan 12, 2012

Subjects & Policy Tags

Policy Area:

Emergency Management

Related Bills

No related bills are listed.

Summary (as of Jul 11, 2012)

Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness Act of 2012 or the PRECISE Act of 2012 - (Sec. 2) Amends the Homeland Security Act of 2002 to direct the Secretary of Homeland Security (DHS) to perform necessary activities to facilitate the protection of federal systems and to assist critical infrastructure owners and operators, upon request, in protecting their critical infrastructure information systems, including by: (1) conducting risk assessments and providing technical assistance; (2) assisting in fostering the development of essential information security technologies and capabilities for protecting federal systems and critical infrastructure information systems; (3) assisting in efforts to mitigate communications and information technology supply chain vulnerabilities; (4) supporting nationwide awareness and outreach efforts to educate the public; and (5) conducting exercises, simulations, and other activities designed to support and evaluate the national cyber incident response plan.

Directs the Secretary, at the direction of the Office of Management and Budget (OMB), to: (1) conduct targeted risk assessments and operational evaluations for federal systems, which may include threat, vulnerability, and impact assessments and penetration testing; (2) provide for the use of consolidated intrusion detection, prevention, or other protective capabilities and associated countermeasures for the purpose of protecting federal systems from cybersecurity threats; (3) assess and foster the development of information security technologies and capabilities for use and dissemination through DHS and to be made available across multiple agencies; (4) designate an entity within DHS to receive reports and information about cybersecurity incidents, threats, and vulnerabilities affecting federal systems; and (5) provide incident detection, analysis, mitigation, and response information and remote or on-site technical assistance for federal systems.

Authorizes the Secretary to acquire, intercept, retain, use, and disclose communications and other system traffic transiting to or from, or stored on, federal systems and to deploy countermeasures with regard to such communications and system traffic for cybersecurity purposes (cybersecurity operational activities) if the Secretary certifies that: (1) such acquisitions, interceptions, and countermeasures are reasonably necessary for protecting federal systems from cybersecurity threats; (2) the content of communications will be collected and retained only when the communication is associated with a known or reasonably suspected cybersecurity threat and communications and system traffic will not be subject to the operation of a countermeasure unless associated with such threats; (3) information obtained pursuant to cybersecurity operational activities will only be retained, used, or disclosed to protect federal systems from cybersecurity threats, to mitigate against such threats, or for law enforcement purposes with the Attorney General's approval when the information is evidence of a crime; (4) notice has been provided to users of federal systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic; and (5) such activities are implemented pursuant to policies and procedures that have been reviewed and approved by the Attorney General.

Authorizes the Secretary to contract with, or request and obtain the assistance of, private entities that provide electronic communication or cybersecurity services to acquire, intercept, retain, use, and disclose communications and other system traffic. Authorizes agencies to permit the Secretary, or a private entity assisting the Secretary, to acquire, intercept, retain, use, or disclose communications, system traffic, records, or other information transiting to or from, or stored on, a federal system for the purpose of protecting federal systems from cybersecurity threats or mitigating such threats in connection with cybersecurity activities.

Provides that no otherwise privileged communication obtained in accordance with, or in violation of, such activities shall lose its privileged character.

Directs the Secretary to designate a lead cybersecurity official within DHS to provide leadership to the cybersecurity

activities of DHS and to ensure that DHS's cybersecurity activities are coordinated with all other DHS infrastructure protection and cybersecurity programs and activities.

Directs the Secretary, in carrying out cybersecurity activities, to: (1) coordinate with relevant federal agencies, state and local government representatives, critical infrastructure owners and operators, suppliers of technology for such owners and operators, academia, and international organizations and foreign partners; and (2) develop and maintain a strategy that articulates DHS actions necessary to assure the readiness, reliability, continuity, integrity, and resilience of federal systems and critical infrastructure information systems. Requires such strategy to: (1) foster the continued superiority and reliability of the U.S. information technology and communications sectors, and (2) ensure that DHS activities are undertaken in a manner that protects statutory privacy rights and civil liberties of U.S. persons.

Requires the Privacy Officer of DHS to review on an ongoing basis, and prepare privacy impact assessments on, the cybersecurity policies, programs, and activities of DHS to ensure compliance with constitutional and legal protections.

Authorizes the Secretary, in order to assure that DHS has the necessary resources to carry out such cybersecurity activities, to: (1) convert competitive service positions to excepted service or establish new excepted service positions within the Office of Cybersecurity and Communications, to carry out cybersecurity functions; and (2) fix compensation for such positions, provide additional forms of compensation, and pay a retention bonus as needed to retain essential personnel. Directs the Secretary to submit to appropriate congressional committees a detailed report that includes: (1) a discussion of the Secretary's use of such flexible authority to recruit and retain qualified employees, (2) metrics on relevant personnel actions, and (3) long- and short-term strategic goals to address critical skills deficiencies.

(Sec. 3) Directs the Secretary to make appropriate cyber threat information obtained by DHS pursuant to National Security Act of 1947 or other information appropriately in the possession of DHS available to appropriate owners and operators of critical infrastructure on a timely basis consistent with the statutory and other appropriate restrictions on the dissemination of such information and with the Secretary's responsibilities under the Homeland Security Act of 2002.

Establishes within DHS the National Cybersecurity and Communications Integration Center, which shall be the primary entity within DHS for sharing timely cyber threat information and exchanging technical assistance, advice, and support with appropriate entities pursuant to DHS's authorities. Requires the Center to have a board of advisors which shall advise the Secretary on Center operations and act as an advocate on behalf of the private sector in improving such operations. Requires the Secretary to develop a charter to govern the operations and administration of the Center, including procedures for making cyber incident information available to outside groups for academic research and insurance actuarial purposes.

Authorizes the Secretary to provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential cybersecurity threats as appropriate.

Authorizes appropriations for FY2013-FY2015 for the administration and management of the Center.

(Sec. 4) Directs the Under Secretary for Science and Technology to support research, development, testing, evaluation, and transition of cybersecurity technology to improve the ability of the United States to prevent, protect against, detect, respond to, and recover from acts of terrorism and cyber attacks, with an emphasis on attacks that would cause a debilitating impact on national security, national economic security, or national public health and safety, including work to: (1) advance the development and deployment of more secure versions of fundamental Internet protocols and architectures; (2) improve, create, and advance the research and development of techniques and technologies for proactive detection and identification of threats, attacks, and terrorist acts before they occur; (3) advance technologies for

detecting attacks or intrusions; (4) improve and create mitigation and recovery methodologies; (5) develop and support infrastructure and tools to support cybersecurity research and development efforts; (6) assist in the development and support of technologies to reduce vulnerabilities in process control systems; (7) develop and support cyber forensics and attack attribution; (8) test, evaluate, and facilitate the transfer of technologies associated with the engineering of less vulnerable software and securing the information technology software development life cycle; (9) ensure new cybersecurity technology is scientifically and operationally validated; and (10) facilitate the planning, development, and implementation of international cooperative activities to address cybersecurity and energy infrastructure with specified foreign entities.

Directs the Under Secretary to coordinate all activities with: (1) the Under Secretary for National Protection and Programs Directorate; and (2) the heads of other relevant federal departments and agencies, academic institutions, the Networking and Information Technology Research and Development Program, and other appropriate working groups established by the President to identify unmet needs and cooperatively support activities.

(Sec. 5) Directs the Secretary to submit a report on support DHS might provide to regional, state, and local grass roots cyber cooperatives, including an analysis of progress in establishing the NET Guard authorized under the Homeland Security Act to build a national technology guard for cyber response capabilities and an assessment of whether a grant process for pilot regional, state, or local cyber cooperatives would be beneficial.

(Sec. 6) Authorizes the Secretary to establish a Cybersecurity Domestic Preparedness Consortium to: (1) provide training to state and local first responders and officials for preparing for and responding to cybersecurity attacks, (2) develop and update a curriculum utilizing the DHS National Cyber Security Division sponsored Community Cyber Security Maturity Model for state and local first responders and officials, (3) provide technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response, and (4) conduct cybersecurity training and simulation exercises to defend from and respond to cyber attacks.

Authorizes the Secretary, as part of the Consortium, to establish one or more cybersecurity training centers. Requires the Consortium to develop a plan to implement as one of the centers a one-year voluntary pilot program to test and assess the feasibility, costs, and benefits of providing cybersecurity training to state and local law enforcement personnel through the national network of fusion centers. Directs the Secretary to implement a one-year voluntary pilot program to train state and local law enforcement personnel in the national network of fusion centers in cyber security standards, procedures, and best practices.

Actions Timeline

- **Sep 21, 2012:** Committee on Energy and Commerce discharged.
- **Sep 21, 2012:** Placed on the Union Calendar, Calendar No. 501.
- **Jul 11, 2012:** Reported (Amended) by the Committee on Homeland Security. H. Rept. 112-592, Part I.
- **Jul 11, 2012:** Committee on Oversight and Government discharged.
- **Jul 11, 2012:** Committee on Science, Space, and Technology discharged.
- **Jul 11, 2012:** Committee on Judiciary discharged.
- **Jul 11, 2012:** Committee on Intelligence (Permanent) discharged.
- **Jul 11, 2012:** Referred sequentially to the House Committee on Energy and Commerce for a period ending not later than Sept. 21, 2012 for consideration of such provisions of the bill and amendment as fall within the jurisdiction of that committee pursuant to clause 1(f) of rule X.
- **Apr 18, 2012:** Committee Consideration and Mark-up Session Held.
- **Apr 18, 2012:** Ordered to be Reported (Amended) by the Yeas and Nays: 16 - 13.
- **Feb 1, 2012:** Subcommittee Consideration and Mark-up Session Held.
- **Feb 1, 2012:** Forwarded by Subcommittee to Full Committee (Amended) by Voice Vote .
- **Jan 12, 2012:** Referred to the Subcommittee on Technology and Innovation.
- **Jan 6, 2012:** Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
- **Jan 4, 2012:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
- **Dec 15, 2011:** Introduced in House
- **Dec 15, 2011:** Referred to the Committee on Homeland Security, and in addition to the Committees on Oversight and Government Reform, Science, Space, and Technology, the Judiciary, and Intelligence (Permanent Select), for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.