HR 6423

Homeland Security Cyber and Physical Infrastructure Protection Act of 2010

Congress: 111 (2009–2011, Ended)
Chamber: House
Policy Area: Emergency Management
Introduced: Nov 17, 2010
Current Status: Referred to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology.
Latest Action: Referred to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. (Nov 23, 2010)
Official Text: https://www.congress.gov/bill/111th-congress/house-bill/6423

Sponsor

Name: Rep. Thompson, Bennie G. [D-MS-2]
Party: Democratic • **State:** MS • **Chamber:** House

Cosponsors (2 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Clarke, Yvette D. [D-NY-11]	D · NY		Nov 17, 2010
Rep. Harman, Jane [D-CA-36]	D · CA		Nov 17, 2010

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security Committee	House	Referred to	Nov 23, 2010
Oversight and Government Reform Committee	House	Referred To	Nov 17, 2010

Subjects & Policy Tags

Policy Area:

Emergency Management

Related Bills

No related bills are listed.

Summary (as of Nov 17, 2010)

Homeland Security Cyber and Physical Infrastructure Protection Act of 2010 - Amends the Homeland Security Act of 2002 to establish within the Department of Homeland Security (DHS) an Office of Cybersecurity and Communications, which shall be headed by the Assistant Secretary for Cybersecurity and Communications and which shall include: (1) the United States Computer Emergency Readiness Team; (2) a Cybersecurity Compliance Division (established by this Act); and (3) other DHS components with primary responsibility for emergency or national communications or cybersecurity.

Directs the Secretary of DHS, acting through the Assistant Secretary or the Director of such Division, to establish and enforce cybersecurity requirements for civilian nonmilitary and non-intelligence community federal systems to prevent, deter, respond to, and recover from cyber attacks and incidents.

Requires the Assistant Secretary to chair an interagency working group, which shall: (1) develop risk- and performance-based cybersecurity requirements for civilian federal agency computer networks and federally owned critical infrastructure, to be enforced by the Assistant Secretary through the Director; (2) develop remedies for noncompliance with such requirements, to be executed by the Director of the Office of Management and Budget (OMB); (3) recommend budgets for security of such networks; and (4) propose updates for the Common Criteria for Information Technology Security Evaluation.

Requires all federal entities to report any cyber incidents on their networks to the Director and to the Team, which shall research each incident and report on the extent of any compromise, the attackers, the method of penetration, the ramifications, and recommended mitigation activities.

Requires: (1) the Secretary, through the Director, to establish and enforce risk-based cybersecurity requirements for private sector computer networks within covered critical infrastructures; and (2) the Director to require entities determined to be covered critical infrastructures to comply with such requirements and to submit a proposed cybersecurity plan to satisfy such requirements to the first-party regulatory agency or sector-specific agency for approval and enforcement. Prescribes penalties for noncompliance.

Requires the Assistant Secretary to: (1) share information regarding cybersecurity threats and vulnerabilities and proposed actions to mitigate them with all federal agencies, appropriate state, local, or tribal authority representatives, and all covered critical infrastructure owners and operators; and (2) designate information received from and provided to federal agencies and critical infrastructure owners and operators under this Act as sensitive security information and enforce requirements for handling, storage, and dissemination of such information.

Directs the Under Secretary for Science and Technology to support research, development, testing, evaluation, and transition of cybersecurity technology, with an emphasis on research and development relevant to large-scale, high-impact attacks.

Requires the Assistant Secretary to: (1) develop a strategic cybersecurity workforce plan as part of the federal agency performance plan; (2) establish a cybersecurity awareness and education curriculum that shall be required for all federal employees and contractors engaged in the design, development, or operation of civilian federal agency computer networks; and (3) implement a strategy to provide federal employees who work in cybersecurity-related areas with the opportunity to obtain additional education.

Authorizes: (1) the appointment of up to 500 employees to carry out this Act's requirements without regard to the civil service laws upon certification to Congress that standard federal hiring processes have not resulted in the required

number of critical cybersecurity positions being filled; and (2) payment of bonuses necessary to retain such an employee.

Actions Timeline

- **Nov 23, 2010:** Referred to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology.
- **Nov 18, 2010:** Sponsor introductory remarks on measure. (CR E1976)
- **Nov 17, 2010:** Introduced in House
- **Nov 17, 2010:** Referred to House Homeland Security
- **Nov 17, 2010:** Referred to the Committee on Homeland Security, and in addition to the Committee on Oversight and Government Reform, 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.
- **Nov 17, 2010:** Referred to House Oversight and Government Reform

LegiList

CONGRESS, MADE CLEAR.

Search Every Federal Bill, Law, and Vote

LegiList is the fastest way to research Congress. Track any bill from introduction to enactment, see how every legislator voted, follow committee activity, and read the full text of every bill — all in one place, always up to date.

legilist.com

Free Course: Learn How Congress Actually Works

LegiList Learn is a free, self-paced course that walks through the entire legislative process — from drafting a bill to a presidential signature. Seven modules, plain language, no politics. Earn a certificate when you finish.

legilist.com/learn

Developer API: Build Apps on Legislative Data

The LegiList API gives developers direct access to bills, votes, legislators, committees, and more. Start free with 1,000 requests per day — no credit card required. Upgrade to Pro when you need to scale.

legilist.com/api

Public data belongs to the public. — legilist.com