S 813

Cyber Security Public Awareness Act of 2011

Congress: 112 (2011–2013, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Apr 13, 2011
Current Status: Sponsor introductory remarks on measure. (CR S2498)
Latest Action: Sponsor introductory remarks on measure. (CR S2498) (Apr 14, 2011)
Official Text: https://www.congress.gov/bill/112th-congress/senate-bill/813

Sponsor

Name: Sen. Whitehouse, Sheldon [D-RI]
Party: Democratic • **State:** RI • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Kyl, Jon [R-AZ]	R · AZ		Apr 13, 2011

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Apr 13, 2011

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

No related bills are listed.

Summary (as of Apr 13, 2011)

Cyber Security Public Awareness Act of 2011 - Directs the Secretary of Homeland Security (DHS) to submit an annual report that: (1) summarizes major cyber incidents involving networks of executive agencies, except for the Department of Defense (DOD); (2) provides aggregate statistics on the number of breaches of networks of executive agencies, the volume of data exfiltrated, and the estimated cost of remedying the breaches; and (3) discusses the risk of cyber sabotage. Requires a similar report by the Secretary of DOD.

Directs: (1) the Attorney General and the Director of the Federal Bureau of Investigation (FBI) to submit reports and annual updates describing investigations and prosecutions by the Department of Justice (DOJ) relating to cyber crimes, resources devoted to the enforcement, investigation, and prosecution of such crimes, and legal impediments to such prosecutions; (2) the Securities and Exchange Commission (SEC) to report on the extent of financial risk to issuers of securities caused by cyber crimes, on any resulting legal liability, and on whether current financial statements of issuers transparently reflect that risk to shareholders; and (3) designated primary regulators responsible for the security of specified critical industries to submit annual reports describing vulnerabilities to, and the prevalence of, cyber attacks for each industry.

Directs the Attorney General, in coordination with the Administrative Office of the United States Courts, to submit a report on: (1) whether federal courts have granted timely relief in matters relating to botnets and other cyber crime and cyber security threats; and (2) recommended changes to the rules of civil or criminal procedure, the resources, capabilities, and specialization of courts to which such cases may be assigned, and federal civil and criminal laws.

Directs the Secretary of DHS to: (1) submit annual reports describing policies and procedures for federal agencies to assist a private sector entity in defending its information networks against cyber threats that could result in loss of life or significant harm to the national economy or national security; (2) contract with the National Research Council or another federally funded research and development corporation for reports on available technical options for enhancing the security of the information networks of entities that own or manage critical infrastructure; (3) submit annual reports on impediments to public awareness of common cyber security threats; (4) submit annual reports on the vulnerability to malicious activity of U.S. telecommunications networks due to the presence of technology produced by foreign suppliers linked to a foreign government; and (5) submit a report on the threat of a cyber attack disrupting the U.S. electrical grid and the national security implications.

Actions Timeline

- **Apr 14, 2011:** Sponsor introductory remarks on measure. (CR S2498)
- **Apr 13, 2011:** Introduced in Senate
- **Apr 13, 2011:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.