S 1638

Cybersecurity Public Awareness Act of 2013

Congress: 113 (2013–2015, Ended)
Chamber: Senate
Policy Area: Government Operations and Politics
Introduced: Oct 31, 2013
Current Status: Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
Latest Action: Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Oct 31, 2013)
Official Text: https://www.congress.gov/bill/113th-congress/senate-bill/1638

Sponsor

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

Cosponsors (3 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Blumenthal, Richard [D-CT]	D · CT		Oct 31, 2013
Sen. Blunt, Roy [R-MO]	R · MO		Oct 31, 2013
Sen. Graham, Lindsey [R-SC]	R · SC		Oct 31, 2013

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Oct 31, 2013

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

No related bills are listed.

Summary (as of Oct 31, 2013)

Cybersecurity Public Awareness Act of 2013 - 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 similar reports by the DOD Secretary to address incidents against DOD and military departments.

Directs 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 instrusions, computer or network compromise, or other forms of illegal hacking. Requires such reports to identify the resources devoted to the enforcement, investigation, and prosecution of such activities and to discuss legal impediments to prosecutions.

Requires the Securities and Exchange Commission (SEC) to submit annually, for three years, a report: (1) assessing the reporting of cyber risk or cyber incidents in financial statements by issuers of securities; and (2) evaluating SEC actions, including staff guidance.

Directs the DHS Secretary to: (1) submit annual reports describing policies and procedures through which federal agencies, upon request, assist in defending a private sector entity's information networks against cyber threats that could result in loss of life or significant harm to the national economy or national security; (2) submit annually, for three years, a report describing vulnerabilities to, and the prevalence of, cyber threats in specified critical infrastructure sectors and the degree to which cooperative activities with DOD-developed private partners have been employed in each sector; (3) contract with the National Research Council or another federally funded research and development corporation for reports on the opportunities for development of new technologies or approaches to enhance the cybersecurity of critical infrastructure entities; and (4) submit annual reports on impediments to public awareness of common cyber security threats.

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 cybercrime and 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.

Actions Timeline

- **Oct 31, 2013:** Introduced in Senate
- **Oct 31, 2013:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.