S 21

Cybersecurity and American Cyber Competitiveness Act of 2013

Congress: 113 (2013–2015, Ended)
Chamber: Senate
Policy Area: Science, Technology, Communications
Introduced: Jan 22, 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. (Jan 22, 2013)
Official Text: https://www.congress.gov/bill/113th-congress/senate-bill/21

Sponsor

Name: Sen. Rockefeller, John D., IV [D-WV]
Party: Democratic • **State:** WV • **Chamber:** Senate

Cosponsors (7 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Carper, Thomas R. [D-DE]	D · DE		Jan 22, 2013
Sen. Coons, Christopher A. [D-DE]	D · DE		Jan 22, 2013
Sen. Feinstein, Dianne [D-CA]	D · CA		Jan 22, 2013
Sen. Levin, Carl [D-MI]	D · MI		Jan 22, 2013
Sen. Mikulski, Barbara A. [D-MD]	D · MD		Jan 22, 2013
Sen. Whitehouse, Sheldon [D-RI]	D · RI		Jan 22, 2013
Sen. Menendez, Robert [D-NJ]	D · NJ		Jan 23, 2013

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Jan 22, 2013

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

No related bills are listed.

Summary (as of Jan 22, 2013)

Cybersecurity and American Cyber Competitiveness Act of 2013 - Calls for the enactment of bipartisan legislation to improve communication and collaboration between the private sector and the federal government to secure the United States against cyber attack, enhance the competitiveness of the United States and create jobs in the information technology industry, and protect the identities and sensitive information of U.S. citizens and businesses by: (1) enhancing the security and resiliency of public and private communications and information networks against cyber attack; (2) establishing mechanisms for sharing cyber threat and vulnerability information between the government and the private sector; (3) developing a public-private system to improve the capability of the United States to assess cyber risk and prevent, detect, and respond to cyber attacks against critical infrastructure such as the electric grid, the financial sector, and telecommunications networks; (4) promoting research and development investments and professional training; (5) preventing and mitigating identity theft; (6) enhancing U.S. diplomatic capacity and public-private international cooperation to respond to emerging cyber threats; (7) expanding resources for investigating and prosecuting cyber crimes in a manner that respects privacy rights and civil liberties and promotes U.S. innovation; and (8) maintaining robust protections of the privacy of U.S. citizens and their online activities and communications.

Actions Timeline

- **Jan 22, 2013:** Introduced in Senate
- **Jan 22, 2013:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.