HR 6183

Cyber Privacy Fortification Act of 2012

Congress: 112 (2011–2013, Ended)
Chamber: House
Policy Area: Science, Technology, Communications
Introduced: Jul 25, 2012
Current Status: Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
Latest Action: Referred to the Subcommittee on Crime, Terrorism, and Homeland Security. (Aug 1, 2012)
Official Text: https://www.congress.gov/bill/112th-congress/house-bill/6183

Sponsor

Name: Rep. Conyers, John, Jr. [D-MI-14]
Party: Democratic • **State:** MI • **Chamber:** House

Cosponsors (2 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Johnson, Henry C. "Hank," Jr. [D-GA-4]	D · GA		Jul 25, 2012
Rep. Scott, Robert C. "Bobby" [D-VA-3]	D · VA		Jul 25, 2012

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	House	Referred to	Aug 1, 2012

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

No related bills are listed.

Summary (as of Jul 25, 2012)

Cyber Privacy Fortification Act of 2012 - Amends the federal criminal code to provide criminal penalties for intentional failures to provide required notices of a security breach involving sensitive personally identifiable information. Defines "sensitive personally identifiable information" to mean specified electronic or digital information.

Defines "security breach" as a compromise of the security, confidentiality, or integrity of computerized data that there is reason to believe has resulted in improper access to sensitive personally identifiable information.

Requires a person who owns or possesses data in electronic form containing a means of identification and who has knowledge of a major security breach of the system containing such data maintained by such person to provide prompt notice to the U.S. Secret Service or Federal Bureau of Investigation (FBI).

Defines "major security breach" as any security breach involving: (1) means of identification pertaining to at least 10,000 individuals reasonably believed to have been acquired, (2) databases owned by the federal government, or (3) means of identification of federal employees or contractors involved in national security matters or law enforcement.

Authorizes the Attorney General (DOJ) and any state attorney general to bring civil actions and obtain injunctive relief for violations of federal laws relating to data security.

Requires federal agencies as part of their rulemaking process to prepare and make available to the public privacy impact assessments that describe the impact of certain proposed and final agency rules on the privacy of individuals.

Sets forth authority for agencies to waive or delay certain privacy impact assessment requirements for emergencies and national security reasons.

Directs federal agencies to periodically review promulgated rules that have a significant privacy impact on individuals or a privacy impact on a substantial number of individuals. Requires agencies to consider whether each such rule can be amended or rescinded in a manner that minimizes any such impact while remaining in accordance with applicable statutes.

Provides access to judicial review to individuals adversely affected or aggrieved by final agency action on any such rule.

Actions Timeline

- **Aug 1, 2012:** Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
- **Jul 25, 2012:** Introduced in House
- **Jul 25, 2012:** Referred to the House Committee on the Judiciary.