HR 104

Cyber Privacy Fortification Act of 2015

Congress: 114 (2015–2017, Ended)
Chamber: House
Policy Area: Science, Technology, Communications
Introduced: Jan 6, 2015
Current Status: Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
Latest Action: Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations. (Jan 22, 2015)
Official Text: https://www.congress.gov/bill/114th-congress/house-bill/104

Sponsor

Name: Rep. Conyers, John, Jr. [D-MI-13]
Party: Democratic • **State:** MI • **Chamber:** House

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Johnson, Henry C. "Hank," Jr. [D-GA-4]	D · GA		Jan 6, 2015

Committee Activity

Committee	Chamber	Activity	Date
Judiciary Committee	House	Referred to	Jan 22, 2015

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

No related bills are listed.

Summary (as of Jan 6, 2015)

Cyber Privacy Fortification Act of 2015

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" as 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 the Federal Bureau of Investigation.

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

Authorizes the Attorney General 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

- **Jan 22, 2015:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
- **Jan 6, 2015:** Introduced in House
- **Jan 6, 2015:** Sponsor introductory remarks on measure. (CR E9)
- **Jan 6, 2015:** Referred to the House Committee on the Judiciary.