HR 4791

Federal Agency Data Protection Act

Congress: 110 (2007–2009, Ended)
Chamber: House
Policy Area: Government Operations and Politics
Introduced: Dec 18, 2007
Current Status: Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governm
Latest Action: Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (Jun 4, 2008)
Official Text: https://www.congress.gov/bill/110th-congress/house-bill/4791

Sponsor

Name: Rep. Clay, Wm. Lacy [D-MO-1]
Party: Democratic • **State:** MO • **Chamber:** House

Cosponsors (2 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Towns, Edolphus [D-NY-10]	D · NY		Dec 18, 2007
Rep. Waxman, Henry A. [D-CA-30]	D · CA		Dec 18, 2007

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Jun 4, 2008
Oversight and Government Reform Committee	House	Discharged from	Apr 16, 2008

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

No related bills are listed.

Summary (as of Jun 3, 2008)

Federal Agency Data Protection Act - (Sec. 3) Defines "personally identifiable information" as any information about an individual maintained by a federal agency, including information about the individual's education, finances, medical, criminal, or employment history, that can be used to distinguish or trace such individual's identity or that is otherwise linked or linkable to the individual.

(Sec. 4) Includes within the information security duties of the Director of the Office of Management and Budget (OMB): (1) reviewing agency information security programs, including plans and schedules, developed on the basis of priorities for addressing levels of identified risk, for conducting testing and evaluation and remedial action to address deficiencies; (2) establishing minimum requirements for the protection of personally identifiable information maintained in or transmitted by mobile digital devices, including requirements for the use of technologies that efficiently and effectively render information unusable by unauthorized persons; (3) requiring agencies to comply with minimally acceptable system configuration requirements consistent with best practices, including checklists developed under the Cyber Security Research and Development Act by the Director of the National Institute of Standards and Technology, and minimally acceptable requirements for periodic testing and evaluation of the implementation of such configuration requirements; (4) ensuring that agency contracts for the provision of information technology products or services include requirements for contractors to meet such configuration requirements; and (5) ensuring the establishment of contract requirements to ensure compliance with this Act with regard to providing security for information and information systems used or operated by an agency contractor or other organization on the agency's behalf.

(Sec. 5) Requires agencies to include in their information security programs: (1) policies and procedures that ensure compliance with minimally acceptable system configuration requirements as required by the Director (currently, the agency); (2) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices as approved by the Director that include testing of systems operated by an agency contractor; and (3) plans and procedures for ensuring the adequacy of information security protections for systems maintaining or transmitting personally identifiable information, including requirements for maintaining a current inventory of such systems, implementing information security requirements for mobile digital devices maintaining or transmitting such information, and developing, implementing, and overseeing remediation plans to address vulnerabilities in information security protections. Allows testing requirements to be satisfied by independent testing, evaluation, or audits.

(Sec. 6) Requires the Director to report to Congress on a summary of information security breaches reported by agencies to the Director and the federal information security incident center.

Requires the Director to oversee the establishment of policies, procedures, and standards for agencies to follow in the event of a breach involving the disclosure of personally identifiable information, specifically including: (1) a requirement for timely notice to those individuals whose information could be compromised, except when the breach does not create a reasonable risk of identity theft, fraud, or other unlawful conduct or of other harm to the individual; (2) guidance regarding whether additional special actions are necessary and appropriate, including data breach analysis, fraud resolution services, identify theft insurance, and credit protection or monitoring services; and (3) a requirement for the timely reporting of such breaches to the Director and federal information security center.

Requires agency heads to delegate to their Chief Information Officer the authority to ensure compliance and to enforce information security requirements, including developing and maintaining an inventory of personal computers laptops or hardware containing personally identifiable information.

Requires agencies to include in their information security programs: (1) procedures for notifying individuals whose personally identifiable information may have been compromised or accessed following a breach; and (2) procedures for the timely reporting of breaches involving personally identifiable information.

Includes among functions of Chief Human Capital Officers the prescription of policies and procedures for exit interviews of employees, including a full accounting of all federal personal property assigned.

(Sec. 7) Requires agency heads to implement expeditiously and revise as necessary a plan to ensure the security and privacy of information collected or maintained by or on behalf of agencies from the risks posed by certain peer-to-peer file sharing programs. Requires the Comptroller General to review and report to specified congressional committees on the adequacy of such plans.

(Sec. 8) Requires audits (currently, evaluations are required) of agency information programs and practices to determine whether information security controls are effective.

(Sec. 9) Amends the E-Government Act of 2002 to require the Director to develop best practices for agencies to follow in conducting privacy impact assessments.

Actions Timeline

- **Jun 4, 2008:** Received in the Senate and Read twice and referred to the Committee on Homeland Security and Governmental Affairs.
- **Jun 3, 2008:** Mr. Clay moved to suspend the rules and pass the bill, as amended.
- **Jun 3, 2008:** Considered under suspension of the rules. (consideration: CR H4853-4856)
- **Jun 3, 2008:** DEBATE - The House proceeded with forty minutes of debate on H.R. 4791.
- **Jun 3, 2008:** Passed/agreed to in House: On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote.(text: CR H4853-4854)
- **Jun 3, 2008:** On motion to suspend the rules and pass the bill, as amended Agreed to by voice vote. (text: CR H4853-4854)
- **Jun 3, 2008:** Motion to reconsider laid on the table Agreed to without objection.
- **May 21, 2008:** Reported (Amended) by the Committee on Oversight and Government. H. Rept. 110-664.
- **May 21, 2008:** Placed on the Union Calendar, Calendar No. 417.
- **Apr 16, 2008:** Subcommittee on Information Policy, Census, and National Archives Discharged.
- **Apr 16, 2008:** Ordered to be Reported (Amended) by Voice Vote.
- **Feb 14, 2008:** Subcommittee Hearings Held.
- **Jan 16, 2008:** Referred to the Subcommittee on Information Policy, Census, and National Archives.
- **Dec 18, 2007:** Introduced in House
- **Dec 18, 2007:** Referred to the House Committee on Oversight and Government Reform.