HR 836

Cyber-Security Enhancement and Consumer Data Protection Act of 2007

Congress: 110 (2007–2009, Ended)
Chamber: House
Policy Area: Crime and Law Enforcement
Introduced: Feb 6, 2007
Current Status: Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
Latest Action: Referred to the Subcommittee on Crime, Terrorism, and Homeland Security. (Mar 1, 2007)
Official Text: https://www.congress.gov/bill/110th-congress/house-bill/836

Sponsor

Name: Rep. Smith, Lamar [R-TX-21]
Party: Republican • **State:** TX • **Chamber:** House

Cosponsors (9 total)

Cosponsor	Party / State	Role	Date Joined
Rep. Chabot, Steve [R-OH-1]	R · OH		Feb 6, 2007
Rep. Coble, Howard [R-NC-6]	R · NC		Feb 6, 2007
Rep. Forbes, J. Randy [R-VA-4]	R · VA		Feb 6, 2007
Rep. Franks, Trent [R-AZ-2]	R · AZ		Feb 6, 2007
Rep. Gallegly, Elton [R-CA-24]	R · CA		Feb 6, 2007
Rep. Goodlatte, Bob [R-VA-6]	R · VA		Feb 6, 2007
Rep. Lungren, Daniel E. [R-CA-3]	R · CA		Feb 6, 2007
Rep. Pence, Mike [R-IN-6]	R · IN		Feb 6, 2007
Rep. Platts, Todd Russell [R-PA-19]	R · PA		Feb 27, 2007

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security Committee	House	Bills of Interest - Exchange of Letters	Dec 5, 2007
Judiciary Committee	House	Referred to	Mar 1, 2007

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

Bill	Relationship	Last Action
110 S 2213	Related bill	**Oct 22, 2007:** Read twice and referred to the Committee on the Judiciary.
110 HR 2290	Related bill	**Jun 25, 2007:** Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.

Summary (as of Feb 6, 2007)

Cyber-Security Enhancement and Consumer Data Protection Act of 2007 - Amends the federal criminal code to: (1) prohibit accessing or remotely controlling a protected computer to obtain identification information; (2) revise the definition of "protected computer" to include computers affecting interstate or foreign commerce or communication; (3) expand the definition of racketeering to include computer fraud; (4) redefine the crime of computer-related extortion to include threats to access without authorization (or to exceed authorized access of) a protected computer; (5) impose criminal penalties for conspiracy to commit computer fraud; (6) impose a fine and/or five year prison term for failure to notify the U.S. Secret Service or Federal Bureau of Investigation (FBI) of a major security breach (involving a significant risk of identity theft) in a computer system, with the intent to thwart an investigation of such breach; (7) increase to 30 years the maximum term of imprisonment for computer fraud and require forfeiture of property used to commit computer fraud; and (8) impose criminal penalties for damaging 10 or more protected computers during any one-year period.

Directs the U.S. Sentencing Commission to review and amend its guidelines and policy statements to reflect congressional intent to increase criminal penalties for computer fraud.

Authorizes additional appropriations in FY2007-FY2011 to the U.S. Secret Service, the Department of Justice, and the FBI to investigate and prosecute criminal activity involving computers.

Actions Timeline

- **Mar 1, 2007:** Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
- **Feb 6, 2007:** Introduced in House
- **Feb 6, 2007:** Referred to the House Committee on the Judiciary.