

## S 2111

### Cyber Crime Protection Security Act

**Congress:** 112 (2011–2013, Ended)

**Chamber:** Senate

**Policy Area:** Crime and Law Enforcement

**Introduced:** Feb 15, 2012

**Current Status:** Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 324.

**Latest Action:** Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 324. (Feb 16, 2012)

**Official Text:** <https://www.congress.gov/bill/112th-congress/senate-bill/2111>

### Sponsor

**Name:** Sen. Leahy, Patrick J. [D-VT]

**Party:** Democratic • **State:** VT • **Chamber:** Senate

### Cosponsors

*No cosponsors are listed for this bill.*

### Committee Activity

*No committee referrals or activity are recorded for this bill.*

### Subjects & Policy Tags

#### Policy Area:

Crime and Law Enforcement

### Related Bills

Bill	Relationship	Last Action
112 HR 4263	Related bill	<b>Jul 10, 2012:</b> Referred to the Subcommittee on Emerging Threats and Capabilities.
112 S 3342	Related bill	<b>Jun 28, 2012:</b> Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 438.
112 S 2151	Related bill	<b>Mar 1, 2012:</b> Read twice and referred to the Committee on Commerce, Science, and Transportation.
112 S 1151	Related bill	<b>Nov 7, 2011:</b> By Senator Leahy from Committee on the Judiciary filed written report. Report No. 112-91. Additional and Minority views filed.

Cyber Crime Protection Security Act - Amends the federal criminal code to make fraud in connection with the unauthorized access of personally identifiable information (in electronic or digital form) a predicate for instituting a prosecution for racketeering.

Increases penalties for fraud and related activity in connection with computers.

Expands the prohibition against trafficking in passwords to include trafficking through any means by which a protected computer may be accessed without authorization.

Imposes criminal penalties for attempts and conspiracies to commit fraud and related activity in connection with computers.

Modifies criminal and civil forfeiture provisions, including requiring certain civil forfeiture seizures and forfeitures to be performed by persons designated for that purpose by the Secretary of Homeland Security (DHS) or the Attorney General (DOJ).

Prohibits, during and in relation to a felony violation of provisions regarding fraud and related activity in connection with computers, intentionally causing or attempting to cause damage to a critical infrastructure computer if such damage results in (or, in the case of an attempt, would, if completed have resulted in) the substantial impairment of the operation of that computer or of the critical infrastructure associated with the computer. Imposes a prison term of between 3 and 20 years, a fine, or both. Prohibits probation for any person convicted of such a violation. Provides for concurrent sentences under specified circumstances.

Excludes from the definition of "exceeds authorized access" for purposes of the prohibition against fraudulent use of computers, access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or nongovernment employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized.

## Actions Timeline

---

- **Feb 16, 2012:** Read the second time. Placed on Senate Legislative Calendar under General Orders. Calendar No. 324.
- **Feb 15, 2012:** Introduced in Senate
- **Feb 15, 2012:** Sponsor introductory remarks on measure. (CR S700-701)
- **Feb 15, 2012:** Introduced in the Senate. Read the first time. Placed on Senate Legislative Calendar under Read the First Time. (text of measure as introduced: CR S701-702)