

S 1568

Cyberterrorism Prevention Act of 2001

Congress: 107 (2001–2003, Ended)

Chamber: Senate

Policy Area: Crime and Law Enforcement

Introduced: Oct 18, 2001

Current Status: Read twice and referred to the Committee on the Judiciary.

Latest Action: Read twice and referred to the Committee on the Judiciary. (Oct 18, 2001)

Official Text: <https://www.congress.gov/bill/107th-congress/senate-bill/1568>

Sponsor

Name: Sen. Hatch, Orrin G. [R-UT]

Party: Republican • **State:** UT • **Chamber:** Senate

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

| Committee | Chamber | Activity | Date |
|---------------------|---------|-------------|--------------|
| Judiciary Committee | Senate | Referred To | Oct 18, 2001 |

Subjects & Policy Tags

Policy Area:

Crime and Law Enforcement

Related Bills

No related bills are listed.

Cyberterrorism Prevention Act of 2001 - Modifies Federal criminal code provisions regarding fraud and related activity in connection with computers. Establishes penalties for intentionally accessing a protected computer without authorization, or exceeding authorized access, thereby causing: (1) loss to one or more persons during any one-year period aggregating at least \$5,000 in value; (2) the modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals; (3) physical injury to any person; (4) a threat to public health or safety; or (5) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

Increases penalties and broadens the scope of provisions regarding computer-related fraud. Includes within the definition of "protected computer" a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

Includes good faith reliance on a request of a governmental entity to preserve evidence among defenses to civil actions relating to a violation of provisions governing access to stored wire or electronic communications.

Requires the Director of the Federal Bureau of Investigation to take appropriate actions to develop at least ten regional computer forensic laboratories and to provide support, education, and assistance for existing laboratories so that such laboratories have the capability to provide forensic examinations regarding seized or intercepted computer evidence relating to criminal activity, to provide training and education regarding computer-related crime for and to assist law enforcement personnel, and to promote sharing of Federal law enforcement computer crime expertise with State and local authorities.

Actions Timeline

- **Oct 18, 2001:** Introduced in Senate
- **Oct 18, 2001:** Sponsor introductory remarks on measure. (CR S10841)
- **Oct 18, 2001:** Read twice and referred to the Committee on the Judiciary.