

S 921

U.S. ICE Act of 2009

Congress: 111 (2009–2011, Ended)

Chamber: Senate

Policy Area: Government Operations and Politics

Introduced: Apr 28, 2009

Current Status: Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (text of mea

Latest Action: Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (text of measure as introduced: CR S4824-4828) (Apr 28, 2009)

Official Text: <https://www.congress.gov/bill/111th-congress/senate-bill/921>

Sponsor

Name: Sen. Carper, Thomas R. [D-DE]

Party: Democratic • State: DE • Chamber: Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Burris, Roland [D-IL]	D · IL		Jul 6, 2009

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security and Governmental Affairs Committee	Senate	Referred To	Apr 28, 2009
Homeland Security Committee	House	Bills of Interest - Exchange of Letters	Sep 22, 2010

Subjects & Policy Tags

Policy Area:

Government Operations and Politics

Related Bills

Bill	Relationship	Last Action
111 HR 4900	Related bill	May 20, 2010: Ordered to be Reported (Amended) by Voice Vote.

United States Information and Communications Enhancement Act of 2009 or the U.S. ICE Act of 2009 - Replaces two subchapters of federal law on information security with provisions to establish in the Executive Office of the President the National Office for Cyberspace (Office) to serve as the principal office for coordinating an assured, reliable, secure, and survivable global information and communications infrastructure and related capabilities.

Requires the Office's director to develop and implement a comprehensive national cyberspace strategy.

Authorizes the Office, notwithstanding any provision of law or policy, to direct the sponsorship of security clearances for federal officers and employees whose responsibilities involve critical national security infrastructure.

Requires the Office to: (1) oversee the implementation of policies, standards, and guidelines on information security; and (2) require agencies to identify and provide appropriate information security protections.

Makes the head of each agency responsible for providing appropriate information security protections.

Requires each agency to have an annual independent information security effectiveness evaluation.

Directs the Secretary of Commerce to prescribe guidelines and compulsory standards for information systems, including national security systems. Allows the President to disapprove or change the guidelines and standards. Allows the Office and the head of an agency to use more stringent standards.

Requires each agency to coordinate with the United States Computer Emergency Readiness Team (US-CERT). Allows US-CERT's director, notwithstanding any law or policy, to direct the sponsorship of the security clearances for federal officers and employees whose responsibilities involve critical national security infrastructure.

Requires the components of each executive branch department or agency (except the Department of Defense or any such component performing any national security function) to establish an automated reporting mechanism allowing its chief information security officer and security operations center at the agency level to implement and monitor the component's security policies, procedures, and controls.

Actions Timeline

- **Apr 28, 2009:** Introduced in Senate
- **Apr 28, 2009:** Sponsor introductory remarks on measure. (CR S4818)
- **Apr 28, 2009:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs. (text of measure as introduced: CR S4824-4828)