# S 3480

Protecting Cyberspace as a National Asset Act of 2010

**Congress:** 111 (2009–2011, Ended)
**Chamber:** Senate
**Policy Area:** Government Operations and Politics
**Introduced:** Jun 10, 2010
**Current Status:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 698.
**Latest Action:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 698. (Dec 15, 2010)
**Official Text:** https://www.congress.gov/bill/111th-congress/senate-bill/3480

## Sponsor

**Name:** Sen. Lieberman, Joseph I. [ID-CT]
**Party:** Democratic • **State:** CT • **Chamber:** Senate

## Cosponsors (2 total)

| Cosponsor | Party / State | Role | Date Joined |
|---|---|---|---|
| Sen. Carper, Thomas R. [D-DE] | D · DE | | Jun 10, 2010 |
| Sen. Collins, Susan M. [R-ME] | R · ME | | Jun 10, 2010 |

## Committee Activity

| Committee | Chamber | Activity | Date |
|---|---|---|---|
| Homeland Security and Governmental Affairs Committee | Senate | Reported By | Dec 15, 2010 |
| 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 5548 | Identical bill | **Sep 13, 2010:** Referred to the Subcommittee on Higher Education, Lifelong Learning, and Competitiveness. |

## Summary (as of Dec 15, 2010)

Protecting Cyberspace as a National Asset Act of 2010 - **Title I: Office of Cyberspace Policy** - (Sec. 101) Establishes in the Executive Office of the President an Office of Cyberspace Policy, which shall: (1) develop a national strategy to increase the security and resiliency of cyberspace; (2) oversee, coordinate, and integrate federal policies and activities relating to cyberspace security and resiliency; (3) ensure that all federal agencies comply with appropriate guidelines, policies, and directives from the Department of Homeland Security (DHS), other federal agencies with responsibilities relating to cyberspace security or resiliency, and the National Center for Cybersecurity and Communications (established by this Act); and (4) ensure that federal agencies have access to, receive, and appropriately disseminate law enforcement, intelligence, terrorism, and any other information relevant to the security of specified federal, military, and intelligence information infrastructure.

(Sec. 102) Requires the President to appoint a Director of Cyberspace Policy.

(Sec. 105) Provides for access by the Director to specified cybersecurity-related information.

(Sec. 107) Requires the Director to submit an annual report describing the activities, ongoing projects, and plans of the federal government designed to meet national strategy goals and objectives.

**Title II: National Center for Cybersecurity and Communications** - (Sec. 201) Amends the Homeland Security Act of 2002 (HSA) to establish within DHS a National Center for Cybersecurity and Communications (NCCC), which shall be headed by a Director, who shall: (1) work cooperatively with the private sector and lead the federal effort to secure, protect, and ensure the resiliency of the federal and national information infrastructure; and (2) work with the Assistant Secretary for Infrastructure Protection to coordinate the information, communications, and physical infrastructure protection responsibilities and activities of NCCC and the Office of Infrastructure Protection. Transfers to NCCC the National Cyber Security Division, the Office of Emergency Communications, and the National Communications System.

Establishes within NCCC the United States Computer Emergency Readiness Team, which shall: (1) collect, coordinate, and disseminate information on risks to specified federal information infrastructure and security controls; and (2) establish a mechanism for engagement with the private sector.

Requires the NCCC Director to: (1) establish a program for sharing information with and between NCCC and other federal agencies; (2) develop guidelines to protect the privacy and civil liberties of U.S. persons and intelligence sources and methods; (3) establish a program to promote and provide technical assistance relating to the implementation of best practices and related standards and guidelines for securing the national information infrastructure; and (4) identify and evaluate the cyber risks to covered critical infrastructure on a continuous and sector-by-sector basis and issue regulations establishing risk-based security performance requirements to secure covered critical infrastructure against cyber risks.

Authorizes the President to issue a declaration of a national cyber emergency to covered critical infrastructure if there is an ongoing or imminent action by any individual or entity to exploit a cyber risk in a manner that attempts to disrupt the operation of the information infrastructure essential to the reliable operation of covered critical infrastructure. Requires the President to notify the owners and operators of the infrastructure of the nature of the emergency, consistent with the protection of intelligence sources and methods. Requires the NCCC Director to take specified steps, including immediately directing the owners and operators to implement required response plans and to ensure that emergency actions represent the least disruptive means feasible to operations.

Prohibits any other federal entity, pursuant to such authority, from: (1) restricting or prohibiting communications over, and not specifically directed to or from, covered critical infrastructure unless the Director determines that no other emergency action will preserve the reliable operation of such infrastructure or the national information infrastructure; (2) controlling covered critical infrastructure; (3) compelling the disclosure of information unless specifically authorized by law; or (4) intercepting a wire, oral, or electronic communication, accessing a stored electronic or wire communication, installing or using a pen register or trap and trace device, or conducting electronic surveillance relating to an incident unless otherwise authorized by specified statutes.

Requires the President to ensure that any declaration or extension is reported to the appropriate congressional committees before the Director mandates any emergency measure or actions. Terminates such an emergency measure or action 30 days after the President's declaration and authorizes extensions for not more than 3 additional 30-day periods under certain conditions if approved by a joint resolution by Congress.

Requires each owner or operator of covered critical infrastructure to certify to the NCCC Director whether the owner or operator has developed and implemented approved security measures and any applicable emergency measures or actions required for any cyber risks and national cyber emergencies. Sets forth civil penalties for violations. Requires the DHS Secretary and the private sector to develop, periodically update, and implement a supply chain risk management strategy designed to ensure the security of the federal information infrastructure.

**Title III: Federal Information Security Management** - (Sec. 301) Sets forth provisions regarding the information security authority and functions of the NCCC Director and executive agency responsibilities. Requires the Director to annually oversee, coordinate, and develop guidance for the effective implementation of operational evaluations of the federal information infrastructure and agency information security programs and practices to determine their effectiveness. Authorizes the Director to order the isolation of any component of the federal information infrastructure if: (1) an agency does not implement measures in an approved risk-based plan; and (2) the failure to comply presents a significant danger to the federal information infrastructure.

Establishes in the executive branch a Federal Information Security Taskforce, which shall be the principal interagency forum for collaboration regarding best practices and recommendations for agency information security and the security of the federal information infrastructure. Requires each agency with an Inspector General appointed under the Inspector General Act of 1978 to assess the adequacy and effectiveness of the information security program and evaluations. Requires the assessments to be performed in accordance with standards developed by the Government Accountability Office, in collaboration with the Council of Inspectors General on Integrity and Efficiency, with assistance from the Taskforce. Provides for the delegation of the Director's authorities to the Secretary of Defense and the Director of the Central Intelligence Agency (CIA) under specified circumstances where unauthorized access, use, disclosure, disruption, modification, or destruction of information would have a debilitating impact on the missions of the Department of Defense (DOD) and the CIA.

**Title IV: Recruitment and Professional Development** - (Sec. 402) Requires the Director of the Office of Personnel Management (OPM) and the NCCC Director to assess the readiness and capacity of the federal workforce to meet the needs of the cybersecurity mission of the federal government. Requires the OPM Director to develop a comprehensive workforce strategy that enhances the readiness, capacity, training, and recruitment and retention of federal cybersecurity personnel. Requires the head of each federal agency to: (1) develop a strategic cybersecurity workforce plan as part of its performance plan; and (2) measure and collect information on indicators of the effectiveness of the recruitment and hiring of a workforce needed to fulfill the agency's cybersecurity mission.

(Sec. 404) Requires the OPM Director, in coordination with: (1) the NCCC Director, to develop and issue comprehensive occupation classifications for federal employees engaged in cybersecurity missions; and (2) the NCCC Director, the Director of National Intelligence, the Secretary of Defense, and the Chief Information Officers Council (CIOC), to establish a cybersecurity awareness and education curriculum that shall be required for all federal employees and contractors engaged in the design, development, or operation of agency information infrastructure.

**Title V: Other Provisions** - (Sec. 501) Amends HSA to direct the Under Secretary for Science and Technology, in coordination with the NCCC Director, to carry out a research and development program for the purpose of improving the security of information infrastructure.

Directs the DHS Secretary to establish a National Cybersecurity Advisory Council to advise the NCCC Director.

(Sec. 502) Amends HSA to direct the Secretary: (1) in establishing and maintaining a prioritized critical information infrastructure list, to consider cyber risks and consequences by sector; (2) to establish and maintain a list of systems or assets that constitute covered critical infrastructure.

Sets forth provisions regarding identification of covered critical infrastructure, compliance with requirements regarding such designation, and development of a process under which an owner or operator of a system or asset that may constitute covered critical infrastructure may request that it be identified as such.

(Sec. 503) Sets forth provisions regarding the use of acquisition authorities by NCCC and a semiannual reporting requirement.

(Sec. 504) Requires the Administrator for Electronic Government and Information Technology, in coordination with CIOC, the Taskforce, and the Council on Inspectors General on Integrity and Efficiency, to evaluate and report on agency adoption and implementation of appropriate information security related policies, memoranda, and directives issued by the Office of Management and Budget (OMB).

## Actions Timeline

- **Dec 15, 2010:** Committee on Homeland Security and Governmental Affairs. Reported by Senator Lieberman with an amendment in the nature of a substitute. With written report No. 111-368.
- **Dec 15, 2010:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 698.
- **Jun 24, 2010:** Committee on Homeland Security and Governmental Affairs. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Jun 10, 2010:** Introduced in Senate
- **Jun 10, 2010:** Sponsor introductory remarks on measure. (CR S4852-4853)
- **Jun 10, 2010:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs.