# HR 85

Terrorism Prevention and Critical Infrastructure Protection Act of 2015

**Congress:** 114 (2015–2017, Ended)
**Chamber:** House
**Policy Area:** Emergency Management
**Introduced:** Jan 6, 2015
**Current Status:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
**Latest Action:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. (Jan 23, 2015)
**Official Text:** https://www.congress.gov/bill/114th-congress/house-bill/85

## Sponsor

**Name:** Rep. Jackson Lee, Sheila [D-TX-18]
**Party:** Democratic • **State:** TX • **Chamber:** House

## Cosponsors (1 total)

| Cosponsor | Party / State | Role | Date Joined |
|---|---|---|---|
| Rep. Cohen, Steve [D-TN-9] | D · TN | | Feb 10, 2015 |

## Committee Activity

| Committee | Chamber | Activity | Date |
|---|---|---|---|
| Homeland Security Committee | House | Referred to | Jan 23, 2015 |

## Subjects & Policy Tags

**Policy Area:**

Emergency Management

## Related Bills

*No related bills are listed.*

## Summary (as of Jan 6, 2015)

**Terrorism Prevention and Critical Infrastructure Protection Act of 2015**

Directs the Secretary of Homeland Security (DHS) to: (1) work with critical infrastructure owners and operators and state, local, tribal, and territorial entities to take proactive steps to manage risk and strengthen the security and resilience of the nation's critical infrastructure against terrorist attacks; (2) establish terrorism prevention policy to engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States; (3) establish a task force to conduct research into the best means to address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect critical infrastructure's interconnectedness and interdependency; (4) establish the Strategic Research Imperatives Program to lead DHS's federal civilian agency approach to strengthen critical infrastructure security and resilience; and (5) make available research findings and guidance to federal civilian agencies for the identification, prioritization, assessment, remediation, and security of their internal critical infrastructure to assist in the prevention, mediation, and recovery from terrorism events.

Directs the Secretary to: (1) appoint a research working group that shall study how best to achieve national unity of effort to protect against terrorism threats and investigate the security and resilience of the nation's information assurance components that provide such protection; and (2) establish a research program to provide strategic guidance, promote a national unity of effort, and coordinate the overall federal effort to promote the security and resilience of the nation's critical infrastructure from terrorist threats.

Sets forth the terrorism protection responsibilities of each federal agency designated for a critical infrastructure sector.

Directs the Secretary to: (1) facilitate the timely exchange of terrorism threat and vulnerability information as well as information that allows for the development of a situational awareness capability for federal civilian agencies during terrorist incidents; (2) implement an integration and analysis function for critical infrastructure that includes operational and strategic analysis on terrorism incidents, threats, and emerging risks; and (3) support greater terrorism cyber security information sharing by civilian federal agencies with the private sector that protects constitutional privacy and civil liberties rights.

Requires a DHS Privacy Officer to be appointed by the President.

Authorizes the Secretary to consult with other federal agencies on how best to align federally funded research and development activities that seek to strengthen the security and resilience of the nation's critical infrastructure.

Requires the Secretary to: (1) develop a description of the functional relationships within DHS and across the federal government related to critical infrastructure security and resilience, (2) analyze the existing public-private partnership model for terrorism information exchange, (3) convene a team of researchers to identify baseline data and systems requirements for such exchange; and (4) demonstrate a near real-time situational awareness, research-based pilot project for critical infrastructure.

Directs the Secretary to provide to the President: (1) a research report that outlines the National Infrastructure Protection Plan to address the implementation of this Act, the requirements of title II of the Homeland Security Act of 2002, and alignment with the National Preparedness Goal and System required by Presidential Policy Directive 8; and (2) a National Critical Infrastructure Security and Resilience Research and Development Plan.

Requires the Secretary to determine which critical infrastructure sectors and agencies should be engaged in efforts to detect, deter, mitigate, and lead recovery efforts related to terrorist incidents.

Directs the National Research Council to evaluate how well DHS is meeting the objectives of this Act.

## Actions Timeline

- **Jan 23, 2015:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
- **Jan 6, 2015:** Introduced in House
- **Jan 6, 2015:** Referred to the House Committee on Homeland Security.