

HR 945

Terrorism Prevention and Critical Infrastructure Protection Act of 2017

Congress: 115 (2017–2019, Ended)

Chamber: House

Policy Area: Emergency Management

Introduced: Feb 7, 2017

Current Status: Referred to the Subcommittee on Cybersecurity and Infrastructure Protection.

Latest Action: Referred to the Subcommittee on Cybersecurity and Infrastructure Protection. (Feb 24, 2017)

Official Text: <https://www.congress.gov/bill/115th-congress/house-bill/945>

Sponsor

Name: Rep. Jackson Lee, Sheila [D-TX-18]

Party: Democratic • **State:** TX • **Chamber:** House

Cosponsors

No cosponsors are listed for this bill.

Committee Activity

Committee	Chamber	Activity	Date
Homeland Security Committee	House	Referred to	Feb 24, 2017
Homeland Security Committee	House	Referred to	Feb 24, 2017

Subjects & Policy Tags

Policy Area:

Emergency Management

Related Bills

No related bills are listed.

Terrorism Prevention and Critical Infrastructure Protection Act of 2017

This bill directs the Department of Homeland Security (DHS) to:

- work with critical infrastructure owners and operators and state, local, tribal, and territorial entities to manage risk and strengthen the security and resilience of the nation's critical infrastructure against terrorist attacks;
- establish terrorism prevention policy to engage with international partners to strengthen critical infrastructure located inside or outside of the United States;
- establish a task force to research the best means to address the security and resilience of critical infrastructure in an integrated, holistic manner;
- establish the Strategic Research Imperatives Program to lead DHS's federal civilian agency approach to strengthen critical infrastructure; and
- provide research findings to federal civilian agencies for the identification, prioritization, assessment, remediation, and security of their internal critical infrastructure.

DHS must: (1) appoint a research working group to study how 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.

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

DHS must: (1) facilitate the timely exchange of terrorism threat and vulnerability information; (2) implement an integration and analysis function for critical infrastructure; and (3) support greater terrorism cyber security information sharing by civilian federal agencies with the private sector.

A DHS Privacy Officer shall be appointed by the President.

DHS must: (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 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.

DHS shall provide to the President a research report that outlines the National Infrastructure Protection Plan and a National Critical Infrastructure Security and Resilience Research and Development Plan.

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

Actions Timeline

- **Feb 24, 2017:** Referred to the Subcommittee on Emergency Preparedness, Response and Communications.
- **Feb 24, 2017:** Referred to the Subcommittee on Cybersecurity and Infrastructure Protection.
- **Feb 7, 2017:** Introduced in House
- **Feb 7, 2017:** Referred to the House Committee on Homeland Security.