# HR 3305

EINSTEIN Act of 2015

**Congress:** 114 (2015–2017, Ended)
**Chamber:** House
**Policy Area:** Government Operations and Politics
**Introduced:** Jul 29, 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. (Aug 11, 2015)
**Official Text:** https://www.congress.gov/bill/114th-congress/house-bill/3305

## Sponsor

**Name:** Rep. Hurd, Will [R-TX-23]
**Party:** Republican • **State:** TX • **Chamber:** House

## Cosponsors (2 total)

| Cosponsor | Party / State | Role | Date Joined |
|---|---|---|---|
| Rep. McCaul, Michael T. [R-TX-10] | R · TX | | Jul 29, 2015 |
| Rep. Ratcliffe, John [R-TX-4] | R · TX | | Jul 29, 2015 |

## Committee Activity

| Committee | Chamber | Activity | Date |
|---|---|---|---|
| Homeland Security Committee | House | Referred to | Aug 11, 2015 |
| Oversight and Government Reform Committee | House | Referred To | Jul 29, 2015 |

## Subjects & Policy Tags

**Policy Area:**

Government Operations and Politics

## Related Bills

| Bill | Relationship | Last Action |
|---|---|---|
| 114 HR 1560 | Related bill | **Jul 14, 2016:** Read twice and referred to the Committee on Homeland Security and Governmental Affairs. |

## Summary (as of Jul 29, 2015)

**EINSTEIN Act of 2015**

Amends the Homeland Security Act of 2002 to require the Department of Homeland Security (DHS) to deploy, operate, and maintain (to make available for use by any federal agency, with or without reimbursement) capabilities to protect federal agency information and federal civilian information systems, including technologies to continuously diagnose, detect, prevent, and mitigate against cybersecurity risks involving such information or systems.

Authorizes the DHS Secretary to access, and allows federal agency heads to disclose to the Secretary, information traveling to or from or stored on such systems, regardless of from where the Secretary accesses such information, notwithstanding any law that would otherwise restrict or prevent such disclosures.

Authorizes the Secretary to retain, use, and disclose information obtained through such activities only to protect federal agency information and federal civilian information systems from cybersecurity risks or in furtherance of the national cybersecurity and communications integration center's (NCCIC's) authority, or, with DOJ approval and if disclosure of such information is not otherwise prohibited by law, to law enforcement only to investigate, prosecute, disrupt, or otherwise respond to:

- criminal computer fraud;
- an imminent threat of death or serious bodily harm;
- a serious threat to a minor, including sexual exploitation or threats to physical safety; or
- an attempt or conspiracy to commit any of such offenses.

Provides liability protections to private entities authorized to assist the Secretary for such purposes.

Redefines for purposes of the NCCIC's cybersecurity functions: (1) "cybersecurity risk" to exclude actions that solely involve a violation of a consumer term of service or a consumer licensing agreement; and (2) "incident" to include an occurrence that actually or imminently jeopardizes, without lawful authority, an information system, thereby replacing a standard that includes occurrences that constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

## Actions Timeline

- **Aug 11, 2015:** Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies.
- **Jul 29, 2015:** Introduced in House
- **Jul 29, 2015:** Referred to the Committee on Oversight and Government Reform, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.