# HR 234

Cyber Intelligence Sharing and Protection Act

**Congress:** 114 (2015–2017, Ended)
**Chamber:** House
**Policy Area:** Armed Forces and National Security
**Introduced:** Jan 8, 2015
**Current Status:** Referred to the Subcommittee on the Constitution and Civil Justice.
**Latest Action:** Referred to the Subcommittee on the Constitution and Civil Justice. (Feb 2, 2015)
**Official Text:** https://www.congress.gov/bill/114th-congress/house-bill/234

## Sponsor

**Name:** Rep. Ruppersberger, C. A. Dutch [D-MD-2]
**Party:** Democratic • **State:** MD • **Chamber:** House

## Cosponsors (3 total)

| Cosponsor | Party / State | Role | Date Joined |
|---|---|---|---|
| Rep. Pittenger, Robert [R-NC-9] | R · NC | | Feb 2, 2015 |
| Rep. Royce, Edward R. [R-CA-39] | R · CA | | Feb 2, 2015 |
| Rep. Brown, Corrine [D-FL-5] | D · FL | | Feb 4, 2015 |

## Committee Activity

| Committee | Chamber | Activity | Date |
|---|---|---|---|
| Armed Services Committee | House | Referred To | Jan 8, 2015 |
| Homeland Security Committee | House | Referred To | Jan 8, 2015 |
| Intelligence (Permanent Select) Committee | House | Referred To | Jan 8, 2015 |
| Judiciary Committee | House | Referred to | Feb 2, 2015 |
| Judiciary Committee | House | Referred to | Feb 2, 2015 |

## Subjects & Policy Tags

**Policy Area:**

Armed Forces and National Security

## Related Bills

*No related bills are listed.*

## Summary (as of Jan 8, 2015)

### Cyber Intelligence Sharing and Protection Act

Directs the federal government to provide for the real-time sharing of actionable, situational cyber threat information between all designated federal cyber operations centers to enable integrated actions to protect, prevent, mitigate, respond to, and recover from cyber incidents.

Directs the President, with respect to information shared by a cybersecurity provider (a non-federal entity that provides goods or services intended to be used for cybersecurity purposes) or self-protected entity (an entity that provides goods or services for cybersecurity purposes to itself), to designate: (1) an entity within the Department of Homeland Security (DHS) as the civilian federal entity to receive cyber threat information, and (2) an entity within the Department of Justice (DOJ) as the civilian federal entity to receive cybersecurity crime information.

Amends the National Security Act of 1947 to require the Director of National Intelligence (DNI) to allow the intelligence community to share cyber threat intelligence with private-sector entities and utilities possessing appropriate certifications or security clearances. Authorizes a cybersecurity provider, with the consent of an entity that contracts with the provider, to: (1) use cybersecurity systems to obtain threat information to protect the rights and property of the contracting entity; and (2) share threat information with any other entity designated by the contracting entity, including DHS and DOJ.

Requires federal agencies receiving shared cyber threat information to establish procedures to: (1) ensure that real-time information is shared with appropriate national security agencies and distributed to other federal agencies; and (2) facilitate collaboration among federal, state, local, tribal, and territorial governments, cybersecurity providers, and self-protected entities.

Directs DHS, the Attorney General, the DNI, and the Department of Defense to establish procedures governing the receipt, retention, use, and disclosure of non-publicly available cyber threat information shared with the federal government.

Sets forth requirements for the use and protection of shared information, including: (1) anonymization or minimization procedures, (2) prohibitions on gaining a competitive advantage, (3) exemptions from public disclosure requirements if information is shared with the government, and (4) prohibitions on the use of such information for regulatory purposes. States that shared information may only be used by a non-federal recipient for a cybersecurity purpose.

Provides civil and criminal liability protections to cybersecurity providers, contracting entities, and self-protected entities acting in good faith to obtain or share threat information or to safeguard systems from threats.

Allows the federal government to use shared cyber threat information for: (1) cybersecurity purposes to ensure the integrity, confidentiality, availability, or safeguarding of a system or network; (2) cybersecurity crime investigations; or (3) protection of individuals from the danger of death or serious bodily harm and the prosecution of crimes involving such danger, including child pornography, sexual exploitation, kidnapping, and trafficking. Prohibits the federal government from affirmatively searching such information for any other purpose.

Repeals amendments made by this Act five years after enactment of this Act.

Expresses the sense of Congress that international cooperation with regard to cybersecurity should be encouraged.

## Actions Timeline

- **Feb 2, 2015:** Referred to the Subcommittee on Crime, Terrorism, Homeland Security, and Investigations.
- **Feb 2, 2015:** Referred to the Subcommittee on the Constitution and Civil Justice.
- **Jan 8, 2015:** Introduced in House
- **Jan 8, 2015:** Referred to the Committee on Intelligence (Permanent Select), and in addition to the Committees on the Judiciary, Armed Services, and 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.