



Cyber Intelligence Sharing and Protection Act

Cybersecurity is an increasingly important issue for U.S. industry, federal and state governmental entities and utilities. It is vital that these entities are able to share cyber threat information in a timely manner. The *Cyber Intelligence Sharing and Protection Act* (CISPA) (H.R. 624) attempts to close gaps in current legislation by improving information sharing for cybersecurity purposes, a goal that AALL strongly supports. Unfortunately, as drafted, H.R. 624 addresses these important issues by including provisions which would allow businesses to share consumer's private information with the government without a warrant or any provisions for significant oversight, while also providing these same companies with protection from liability.

Section 2 of H.R. 624 not only exempts companies which provide information to the federal government from complying with Freedom of Information Act (FOIA) requests, it also places restrictions on how or if cyber threat information voluntarily disclosed by these companies can be shared with Congress or the public. CISPA would also authorize Internet service providers and other companies to share customer communications and other personally identifiable information with governmental agencies, including the National Security Agency. The bill includes a very broad, almost unlimited definition of the information that can be shared with government agencies notwithstanding privacy and other laws, which would likely lead to the expansion of the government's role in the monitoring of private communications as a result of this sharing. Once the information is shared with the government, the information could be used for any purpose that is not specifically prohibited, including for "national security," not just computer and network security.

The *Cyber Intelligence Sharing and Protection Act* threatens the civil liberties and privacy of Americans. AALL urges members of the House of Representatives to oppose CISPA (H.R. 624) because:

- **CISPA would create a gaping new exemption to existing privacy law.** As drafted, CISPA would allow businesses to share consumer's private information with the government without a warrant or any provisions for significant oversight.
- **CISPA constitutes a wholesale attack on public access to information under FOIA.** CISPA unwisely and unnecessarily cuts off all public access to cyber threat information before the public and Congress has the chance to understand the types of information that are withheld under the bill.
- **CISPA will not protect the public from cyber attacks.** As drafted, CISPA limits access to and sharing of cyber threat information disclosed under this legislation, potentially increasing our vulnerability to cyber attacks.