

KEY VOTE ALERT!

October 22, 2015



U.S. CHAMBER OF COMMERCE
Congressional & Public Affairs
1615 H Street, NW
Washington, DC 20062
202-463-5600

TO THE MEMBERS OF THE UNITED STATES SENATE:

The U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, supports the substitute or managers' amendment (#2716) to S. 754, the "Cybersecurity Information Sharing Act of 2015" (CISA).

The Chamber urges the Senate to pass CISA expeditiously. The Select Committee on Intelligence favorably reported CISA by a vote of 14–1 in March, signifying robust bipartisan support for the bill. CISA goes far in addressing the legal and policy cybersecurity priorities that the Chamber has been advocating for several years.

Senators Burr and Feinstein, the authors of CISA, have made significant revisions to CISA by incorporating several of the amendments filed to the underlying bill into a managers' amendment. In addition to the substantive privacy protections added to the legislation during the committee markup and this summer, the managers' amendment features enhanced oversight reporting requirements to further guard individuals' privacy and civil liberties. The measure ensures that private sector sharing is strictly voluntary, and it includes a review of federal computers with access to personally identifiable information (PII). The managers' amendment also provides for positive outreach to small businesses.

Contrary to the mistaken claims of opponents who seek to conflate this bill with legislation pertaining to government surveillance, CISA does not give the government any new authority to collect data on or surveil individuals, such as for targeting crimes unrelated to cybersecurity.

The Chamber urges Congress to send a bill to the president that gives businesses legal certainty that they have strong protections from liability when voluntarily sharing and receiving threat indicators (CTIs) and defensive measures in real time and monitoring their networks to mitigate cyberattacks. The legislation also needs to offer safeguards related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of information among multiple companies and government agencies and departments.

The Chamber believes that legislation needs to protect privacy and civil liberties and establish appropriate roles for civilian and intelligence agencies, which CISA would do. CISA contains provisions reflecting commonsense negotiations among many stakeholders on these issues.

The Chamber opposes the adoption of amendments that would jeopardize the legal certainty and related industry safeguards provided in the bill. Amendments should not bog down the sharing of CTIs from businesses to the federal entities that need them in a timely manner to protect American communities. Also, changes to the bill should not alter the carefully crafted definitions of “cybersecurity threat” and CTIs, which could lead to frivolous litigation.

Cyberattacks aimed at U.S. businesses and government entities are being launched from various sources, including sophisticated hackers, organized crime, and state-sponsored groups. These attacks are advancing in scope and complexity. Most policymakers and practitioners appreciate that the intent of legislation is not to spur more information sharing for its own sake. Rather, the goal is to help companies achieve timely and actionable situational awareness to improve the business community’s and the nation’s detection, mitigation, and response capabilities.

Additional positive side effects of enacting cyber information-sharing legislation include strengthening the security of personal information that is maintained on company systems and increasing costs on nefarious actors. CISA would complement the cybersecurity framework, which many industry associations and companies developed with the National Institute of Standards and Technology (NIST) and are embracing and promoting with their business partners. Congressional action on cybersecurity information-sharing legislation cannot come quickly enough.

The Chamber has provided the Senate with significant feedback regarding CISA and related amendments and appreciates the extraordinary work that Chairman Burr and Vice Chairman Feinstein, their staff members, and other offices have put into passing CISA. The managers’ amendment includes provisions dealing with federal reporting requirements impacting certain U.S. critical infrastructure entities, which could be challenging for the business community to accept in a final bill. Nevertheless, the Chamber looks forward to working with the relevant lawmakers and committees to address these issues before legislation is sent to the president for signing.

The Chamber strongly supports CISA and urges you to vote in favor of S. 754.
The Chamber may consider votes on, or in relation to, this legislation—including on the motion to invoke cloture—in its annual *How They Voted* scorecard.

Sincerely,

A handwritten signature in black ink, appearing to read "R. Bruce Josten". The signature is fluid and cursive, with the first name "R." and last name "Josten" clearly visible.

R. Bruce Josten