

CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

R. BRUCE JOSTEN
EXECUTIVE VICE PRESIDENT
GOVERNMENT AFFAIRS

1615 H STREET, N.W.
WASHINGTON, D.C. 20062-2000
202/463-5310

November 19, 2014

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, urges the Senate to pass S. 2588, the "Cybersecurity Information Sharing Act of 2014" (CISA), and other important cyber bills before the end of the 113th Congress.

Passing CISA is the Chamber's top cybersecurity legislative priority. S. 2588 would enhance the protection and resilience of businesses' information networks and systems against increasingly sophisticated and malicious actors. This bill would complement the positive National Institute of Standards and Technology (NIST)-coordinated cybersecurity framework, which many business associations and companies are embracing and promoting with their constituents.

Public policy needs to better help American businesses, which are bearing the brunt of cyber attacks coming from foreign powers or their surrogates, organized criminals, and rogue individuals. S. 2588 would help companies achieve timely and actionable situational awareness to improve the business community's and the nation's detection, mitigation, and response capabilities. This bill would also strengthen the security of personal information that is maintained on company networks and systems.

Businesses stress that they need practical safeguards to increase their information-sharing capabilities. CISA's targeted protections—including limited liability, disclosure, and antitrust—would constructively influence businesses' decisions to share cyber threat data and countermeasures more quickly and frequently.

CISA is one of several cyber measures that needs to be passed expeditiously. Here are specific bills that should move with S. 2588:

- S. 1353, the "Cybersecurity Act of 2013," which would authorize NIST to work with industry on an ongoing basis to develop voluntary guidelines and best practices to reduce cyber risks to the U.S. business community;
- S. 2354, the "DHS Cybersecurity Workforce Recruitment and Retention Act of 2014," which would help federal officials hire and retain top cybersecurity talent;

- S. 2519, the “National Cybersecurity and Communications Integration Center Act of 2014,” which would write into law the existence of the Department of Homeland Security’s National Cybersecurity and Communications Integration Center (NCCIC)—a central civilian information-sharing hub for cybersecurity activities. Importantly, CISA would rely heavily on the NCCIC to serve as the primary federal portal for exchanging cyber threat data between government and businesses; and
- S. 2521, the “Federal Information Security Modernization Act of 2014,” which would update the Federal Information Security Management Act of 2002, spurring agencies and departments to improve their security by leveraging automated and continuous monitoring of federal computer networks and systems.

Cyber threats against U.S. businesses and national security are advancing in scope and skill. It would be a significant blow both to industry and its government partners if the Senate fails to pass CISA and these other vital cyber measures—all of which have been reported out of their respective committees with strong bipartisan support. The Chamber urges the Senate to take up these cybersecurity bills and pass them without further delay.

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" being the most prominent parts.

R. Bruce Josten