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

April 22, 2015

TO THE MEMBERS OF THE U.S. HOUSE OF REPRESENTATIVES:

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 H.R. 1560, the Protecting Cyber Networks Act (PCNA), and H.R. 1731, the National Cybersecurity Protection Advancement Act (NCPAA) of 2015. The Chamber urges the House to pass the bills this week.

PCNA and NCPAA were recently reported out of the Permanent Select Committee on Intelligence and the Homeland Security Committees, respectively, with strong bipartisan support. Both measures go far in addressing the legal and policy cybersecurity priorities that the Chamber has been advocating for several years.

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 data indicators and defensive measures in real time and taking actions to mitigate cyberattacks. The legislation also needs to offer safeguards related to public disclosure; regulatory, including the direct and indirect use of information; and anti-trust matters in order to increase the timely exchange of information among multiple companies and government agencies and departments.

It is important to highlight that the Chamber supports linking liability protection to the operation of defensive measures (DMs). This protection is logical, since such measures are clearly preventative, not offensive, in nature and intent. Our organization believes that legislation needs to protect privacy and civil liberties and establish appropriate roles for civilian and intelligence agencies, which NCPAA and PCNA do. Both bills contain provisions reflecting commonsense negotiations among many stakeholders on these issues.

The Chamber opposes the adoption of amendments that would weaken or overly complicate NCPAA or PCNA, including issues related to data security, breach notification, and commercial privacy, which are best addressed in other contexts.

The Chamber provided the Homeland Security and Intelligence committees with comments and recommendations regarding NCPAA and PCNA. We appreciate the solid progress that Chairmen McCaul and Nunes and their staffs have made. Ideally, the House would

make additional changes to create a bidirectional information-sharing program that is more workable in execution.

- **A sunset provision does not factor in the substantial resources required to sustain an information-sharing program. The sunset should be dropped from legislation.** Yesterday, the Rules Committee approved an amendment made in order that would sunset the cybersecurity information-sharing programs established under NCPAA and PCNA after seven years. A sunset provision would almost certainly inhibit businesses' ability to make long-term planning decisions related to risk management and information-sharing investments—which policymakers should want businesses to regularly undertake.

  A sunset provision would imperil businesses' security and resilience if threat-sharing systems are turned off because of lapsed authorizations and related safeguards, such as liability protection. Companies cannot easily turn on their information-sharing infrastructures because the time, logistics, and costs associated with establishing them can be significant. Given the persistence and speed of cyberattacks, a sunset provision is unwise policy, and the Chamber opposes it.

- **PCNA and NCPAA put insufficient emphasis on advancing government-to-business sharing; there should be parity in timely, bidirectional sharing.** The Chamber believes that the information-sharing discussion puts insufficient emphasis on advancing government-to-business sharing. The Chamber urges the bill writers to have federal agencies and departments adopt information-sharing procedures pushing them to send timely, actionable data back to any private entity, including businesses, information sharing and analysis centers (ISACs), and information sharing and analysis organizations (ISAOs). Cyber threat indicators (CTIs) and DMs shared with the government by both private and federal entities need to flow back to businesses at Internet speeds to help those businesses counter future cyberattacks in all but the most extraordinary circumstances.

- **Businesses should be protected when sharing cyber threat information with government agencies and departments authorized in PCNA.** Legislation needs to both authorize and protect businesses that share CTIs and DMs both with any private entity and certain federal government agencies and departments. The Chamber continues to believe that the Department of Homeland Security (DHS)—or any federal entity, for that matter—should not be the sole civilian and protected entity to receive cyber threat data.

  The Chamber supports the flexible approach taken by the House Intelligence committee bill, PCNA, which authorizes and protects businesses when they share cyber threat information with the departments of Commerce, Energy, Homeland Security (Secret Service), Justice (the FBI), Treasury, and the Office of the Director of National Intelligence. After all, with the recent creation of the Cyber Threat Intelligence Integration Center (CTIIC)—which is meant to connect the cyber dots among various federal departments and agencies—it makes little sense to establish in law that DHS

would be the only recipient of protected cyber threat information coming from the private sector.

Worth noting, neither PCNA nor NCPAA protect businesses that share CTIs and DMs with the Department of Defense (DOD), including the National Security Agency (NSA). Despite the disincentive to share with DOD/NSA, the Chamber assumes that policymakers will make robust efforts to access, analyze, and disseminate cyber threat data—much of it gathered at taxpayers' expense—to public and private entities and not leave it in a compartmentalized channel, whether located at DHS, the FBI, or another government entity.

- **The bills' "removal of personal information" or minimization requirements would disadvantage small and midsize businesses (SMBs), creating a disincentive to share. The "reasonable" scrubbing standard would undercut the intent of information-sharing legislation.**
  The bills' call for personal information to be removed by businesses that share CTIs would likely have the unintended consequence of preventing SMBs, and even some large enterprises, from voluntarily participating in an information-sharing program.

  The Chamber urges businesses to share cybersecurity threat data with industry partners and the government. However, the mandate would almost certainly sideline SMBs, because the provision assumes that businesses would have the technical know-how or the resources to scrub data. To be sure, this outcome is not the intent of the bill writers but is the likely response that many businesses would have to this provision.

  Further, the Chamber supports the minimization language found in S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015, which was carefully negotiated over a lengthy period among stakeholders. Specifically, section 4(d)(2) of CISA says, "An entity sharing a cyber threat indicator pursuant to this Act shall, prior to such sharing—(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity *knows at the time of sharing* to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information . . ." (emphasis added).

  In contrast to the Senate bill, PCNA and NCPAA use the vague "reasonable" phrasing to direct the minimization or scrubbing of personal information from CTIs before they are shared. Troubling to the Chamber, the apparently simple concept of "reasonable" is certainly not simple when argued over by competing attorneys, security professionals, and government officials. Thus, use of the language such as "reasonable efforts" and "reasonably believed" in legislation would be an invitation to legal wrangling and contrary to the goal of real-time information sharing—two outcomes that are diametrically opposed to the intent of cyber information-sharing legislation.

Passing an industry-supported information-sharing bill is the Chamber's top cyber legislative priority in 2015

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. PCNA and NCPAA would complement the NIST cybersecurity framework, which many industry associations and companies are embracing and promoting with their business partners. Congressional action on cybersecurity information-sharing legislation cannot come quickly enough. **The Chamber supports PCNA and NCPAA and may consider votes on, or in relation to, these bills in our annual *How They Voted* scorecard.**

Sincerely,

R. Bruce Josten