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

May 19, 2016

The Honorable Lindsey Graham
Chairman
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Sheldon Whitehouse
Ranking Member
Subcommittee on Crime and Terrorism
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Graham and Ranking Member Whitehouse:

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, writes to express its support for your legislation, S. 2931, the "Botnet Prevention Act of 2016." The Chamber supported adding a version of this legislation to cybersecurity information sharing legislation last year.

Businesses' threat detection, information sharing, and incident response capabilities are improving. However, the Chamber urges policymakers to increase the costs on attackers. Law enforcement can point to notable successes in indicting members of overseas criminal networks and partnering with the private sector to disrupt botnets and other malicious activity. But organizations perpetrating such acts are not fearful of attribution, extradition, and prosecution to the degree that it seriously impacts their cost/benefit calculations.

S. 2931 would enhance the Department of Justice's (DOJ's) ability to fight networks of compromised computers known as botnets. Under current law, DOJ's authority to obtain injunctive relief to shut down botnets is limited to botnets engaged in fraud or illegal wiretapping. The legislation would expand DOJ's authority and allow for injunctions against botnets engaged in a broader range of illegal activity, including destruction of data, denial of service attacks, and other criminal acts that cause damage to computers.

The legislation would also give judges the discretion to impose tougher penalties on those who knowingly cause damage to computers that control critical infrastructure systems, without imposing mandatory minimums.

Further, S. 2931 would amend the law to prohibit selling the "means of access" to a compromised computer if the seller knows or has reason to know the buyer intends to cause damage to the computer, use the means of access to commit wire fraud, or violate the criminal

spam statute. This provision would target those who sell access to the compromised computers within a botnet.

Under current law, it is difficult to prosecute sellers of access to compromised computers, particularly when the seller is not the person who compromised the computer in the first place. No current criminal law directly prohibits such conduct. S. 2931 would close this loophole.

Big picture: Cybercrimes are seemingly becoming more routine, more sophisticated, and more alarming. Law enforcement is working diligently to bring domestic and foreign attackers to justice, which the Chamber applauds. The Chamber's national cybersecurity campaign urges businesses to adopt sound Internet security practices to reduce network and system weaknesses and make the price of successful hacking increasingly steep. FBI and Secret Service agents participate at each of the Chamber's national cybersecurity events, and the Chamber urges businesses to report cyber incidents and online crime to government authorities.

Private sector organizations are using the joint industry-National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, creating new resources to help their constituencies reduce risks to their cybersecurity, and sharing best practices through formal and informal means. Industry is also working with government entities to strengthen their information networks and systems against malicious actors.

The Chamber supports increasing the resources that law enforcement agencies need to counter and mitigate cyber threats, including investigating and prosecuting cybercrime cases internationally. S. 2931 would help tip the scales of justice toward American law enforcement and industry.

Sincerely,

R. Bruce Josten

cc: Members of the Committee on the Judiciary