IMPERVA

3400 Bridge Parkway
Suite 200
Redwood Shores
California, 94065

650.394.9000 *tel*
650.345.9004 *fax*

February 12, 2018

U.S. Department of Commerce
1401 Constitution Avenue NW
Washington DC, 20230

Department of Homeland Security
245 Muray Lane, SW
Washington, DC 20528

Dear Secretaries:

Thank you for the invitation to comment on *A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*. The Imperva security research team has tracked botnet and DDoS activity for over a decade and reiterates your findings that DDoS attacks represent one of the most significant impediments to digital commerce.

Imperva launched a worldwide commercial anti-DDoS service in 2011. Based on a software-defined network and the principle of a community defense, over 6,000 enterprise and government organizations have joined the network to protect themselves against DDoS attacks. In late-2016, Imperva mitigated one of the largest documented botnet-initiated DDoS attacks, peaking at over 650 megabits per second. The attack was mitigated among multiple data centers on the west coast of the United States with no impact on any of our clients.

DDoS attack patterns change continuously as the attackers adapt their techniques to mitigation measures. The large sustained attacks of the past have been supplanted by short burst attacks that are designed to render hybrid approaches obsolete. The emergent "pulse wave" attack method reduces attack costs by increasing the number of simultaneous targets while attempting to thwart hybrid and on-premises mitigation measures.

We believe that the most effective and lowest cost anti-DDoS defense is the shared network defense approach for the following reasons:

- Large global-scale networks can be built to absorb multi-terabit attacks and high packet rate attacks that would be prohibitive for any organization to build on their own.
- A large global community of organizations under the protection of the network affords attack intelligence that can be analyzed to predict and mitigate new attack types, like pulse wave, before they inflict damage.
- Software-defined networks can be built to automate mitigation and eliminate the need to deploy on-premises equipment or hybrid systems to monitor or manage DDoS attacks.

- A shared defense offers the lowest cost per organization, and as more organizations join the network, costs may decrease further leading to wider adoption.

Imperva is pleased to continue to play a role in defending our clients against debilitating DDoS attacks while predicting and solving the future threat. We look forward to a public-private working relationship that develops solutions to broaden the effectiveness and adoption of anti-DDoS measures.

Sincerely,

Terry Ray
Chief Technology Officer
Imperva, Inc.
terry@imperva.com