Before the:

National Telecommunications and Information Administration

United States Department of Commerce

Public Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats

Document Citation 83 FR 1342

Docket No. 180103005-8005-01

COMMENTS OF THE INTERNET INFRASTRUCTURE COALITION

February 12, 2018

Submitted by:

Christian Dawson, Executive Director

i2Coalition

718 7th Street, NW

2nd Floor

Washington, DC 20001 (202) 780-7237

I. **INTRODUCTION**

Thank you for the opportunity to present our comments regarding the National Telecommunications and Information Administration's (NTIA) "Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats."

The Internet Infrastructure Coalition (i2Coalition) was founded in 2012 by a diverse group of Internet infrastructure companies to be an effective advocate for those entities that provide the services necessary for the Internet to function and help keep the Internet open, free, and secure. Since our founding, we have made great strides on initiatives that affect our industry and the Internet as a whole—including on issues regarding online threats—and have grown to become the leading voice for the Internet infrastructure community and relevant stakeholders.

Our 90-plus members include web hosting companies, data centers, domain registrars, security companies, software vendors, and other infrastructure-related businesses. Our members range in size from household names such as Google and GoDaddy to small businesses such as HandyNetworks, based in Colorado, and Open Spectrum Inc., based in North Carolina.

II. **GENERAL FEEDBACK**

We are thankful that NTIA took a thoughtful approach to how they document a path forward on botnet recommendations. While botnets present a concern for the federal government, and a threat to the Internet's infrastructure, we believe that this draft acknowledges that abuse is a problem that will never actually be "solved," only mitigated. We strongly believe that only a global, adaptive, market-driven process for mitigation will ultimately be effective. Our ecosystem has natural incentives to continually improve security, and we are doing so. This draft seems to trust the natural evolution of the market, and looks for ways that the federal

government can engage industry in its efforts to minimize the threat landscape throughout the ecosystem, but also at the governmental level.

We feel the federal government should continue to play the role of facilitator and educator. From a practical perspective, departments and agencies have extensive contacts and networks to access and promote collaboration, like with this very report. Government can urge fora, events to share information and moderate discussions about solution development among industry participants. Education will help throughout the process - from publicizing collaboration workshops and publishing best practices and finalized solutions.

III. **IDENTIFICATION OF CONCERNS**

a. **Monoliths -** The Internet infrastructure community's most significant concern is that certain terms used throughout the document are so broad, and not defined within the document, to the point that it is difficult to point to tangible next steps. The terms "government," "cybersecurity community," and "industry" are very broad monoliths. Without further narrowing, we question how the engagements requested can be effectively actionable.

b. **"Should" -** The extremely broad terminology used to describe stakeholders is particularly problematic when coupled with the fact that Section III of the document, Goals & Actions, employs liberal use of the imperative "should" when pointing out how these broad entities are to resolve future issues. Somehow, the document must find resolution to the core issue that broad monoliths are practically unable to take on narrow imperatives. As such, the document either needs to better define the term "should," or it needs to be more specific about who needs to engage with whom.

c. **"Information Sharing" -** In one specific area, a lack of clarity in defining terms might lead industry into a particularly difficult mismatch of what expectations are versus what can realistically be done. The term "Information Sharing" needs to be be better defined. Contextually, we may even suggest "Incident Reporting" as a better alternative, that more accurately reflects the scope of the information.

   It is important to note that there is a great deal of business risk inherent in any type of information sharing, either among corporations or with governments. Privacy violations are only one of many concerns. Strategic, narrow, relationship-driven information sharing programs do exist within industry, but there are practical reasons why global, holistic venues have not been developed to institutionalize that throughout industry. Additionally, the provision of data should be highly controlled with organizations disseminating to parties, e.g., law enforcement, rather than data being pulled from organizations.

   Certainly more can be done among trusted parties through targeted programs, but their scope needs to be narrow and purpose built. Moreover, a secure venue needs to be determined, and clearly articulated fields of data defined before any broad sharing could ever be accomplished. Finally, the cost of this effort must also be considered. The sharing venue must be streamlined to encourage and accommodate participation from organizations large and small.

d. **Centralization As A Threat -** With the increase in centralization of data, cloud-based service offerings and the vast Software As A Service (SaaS) sector also warrant consideration for the scope of this analysis.

e. **Global, Diverse Scope -** It is important to acknowledge that botnets are a global issue, and that no solution will be effective if only U.S. industry players are at the table.

Moreover, the majority of the corporations who operate DNS infrastructure are small or medium sized businesses. No solution on an issue like incident reporting will be effective unless the methods defined for it are able to scale down to an operable size for small business.

f. **Planned Obsolescence** - While a complicated issue to tackle, the presence of issues like "Spectre" demonstrate the need for solutions for aging hardware. We recommend you consider suggestions on how the government can facilitate dialogue on this complex but important topic.

Thank you again for this opportunity to present our thoughts. If you have comments, concerns, or questions about this particular response, i2Coalition looks forward to hearing from you. Moreover, the i2Coalition stands ready to continue to be active in engaging on this critical issue, beyond our comments herein.