Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Promoting Stakeholder Action Against	)	Docket No. 180103005-8005-01
Botnets and Other Automated Threats	)	

COMMENTS OF USTELECOM ASSOCIATION

Robert Mayer
Senior Vice President, Cybersecurity
601 New Jersey Avenue, NW
Suite 600
Washington, DC 20001
(202) 326-7300

February 12, 2018

TABLE OF CONTENTS

Before the
DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Promoting Stakeholder Action Against	)	Docket No. 180103005-8005-01
Botnets and Other Automated Threats	)	

COMMENTS OF THE USTELECOM ASSOCIATION

The USTelecom Association is pleased to comment on the National Telecommunications and Information Administration's (NTIA) Request for Comment (RFC) on the Draft Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and other Automated, Distributed Threats.[1]

In summary, we recommend the following concrete, actionable next steps in the coming months and/or for the Final Report to the President:

1. The Administration should build on the model of well-coordinated, government-convened, private sector activities that has characterized this process thus far, funded and resourced for the long-term.
2. Building on the findings of this initiative to date regarding promoting stakeholder action, NTIA, the National Institute of Standards and Technology (NIST), and the Department of Homeland Security (DHS) should convene industry to determine the specific actions that various stakeholders of all types should take to "share

[1] Department of Commerce, National Telecommunications and Information Administration, *Promoting Stakeholder Action Against Botnets and Other Automated Threats*, Request for Comments, 83 Fed. Reg. 1,342 (January 11, 2018) ("RFC").

responsibility" in addressing distributed, automated threats, and the mechanisms through which those actions will be taken.

3. Regarding device security, NTIA, NIST, and DHS, with the support of the Federal Trade Commission (FTC) and other agencies as needed, should convene industry leaders to promote market awareness of developing solutions. Additionally, the Administration should implement Draft Report Action 1.1 to develop Cybersecurity Framework profiles for the Internet of Things (IoT) devices in various verticals (e.g., auto, healthcare, consumer, etc.).
4. The Communications Sector Coordinating Council (CSCC) proposes to work with DHS, with the active support of NTIA, NIST, the Federal Communications Commission (FCC), the Department of Justice (DOJ) and other agencies as needed, to produce an in-depth report on actions that Internet service providers (ISPs) or network services providers should take in partnership with government, law enforcement, and other stakeholders to advance the resilience of the Internet and communications ecosystem. This report will address the challenges facing smaller ISPs.
5. NTIA, NIST, and DHS, with the support of the Department of State (DOS), the Department of Defense (DOD) and the DOJ, should convene industry to develop a coordinated approach to these challenges among allied governments and market economies such as the United Kingdom and other key allies.

These recommendations are discussed in greater detail below.

I. USTELECOM STRONGLY SUPPORTS THE INDUSTRY-DRIVEN PROCESS UNDERLYING THE DRAFT REPORT.

USTelecom believes that industry-driven processes should be at the heart of cybersecurity policymaking. We therefore applaud the Administration for undertaking such a process aimed at reducing malicious botnets and other distributed and automated cyber threats. The process so far has emphasized private sector operational experience and expertise, and the importance of harnessing market drivers for innovative security solutions. We strongly support the Administration's decision to frame the government's role to be that of a convener, empowering the private sector to take the lead, with clear, navigable interagency coordination and roles for the three lead agencies – NTIA, NIST and DHS – as well as limited but valuable roles for the FTC, the FCC, the DOJ, and other agencies.

We strongly support this model for cybersecurity policymaking, and as we detail in our recommendations below, we urge the Administration to build out on this process in several subsequent initiatives leading up to and following the Final Report in May. USTelecom and its members are already taking significant complementary actions of our own and we anticipate more activity in the coming weeks, and we have high expectations that the Administration will double down on orienting its future cybersecurity efforts around the collaborative model it has advanced in this process. As we state below, this should include sufficient funding and staffing over the long term to sustain this positive momentum for concrete, actionable, innovative advances in cybersecurity.

II. THE DRAFT REPORT PROPERLY REFLECTS THE GOAL OF SHARED RESPONSIBILITY, BUT MORE CLARITY AND SPECIFICITY IS NECESSARY REGARDING ROLES IN THE ECOSYSTEM.

A. SHARED RESPONSIBILITY

The concept of "shared responsibility" on a global market and ecosystem-wide basis is critical in this context and is appropriately reflected in the draft report. The challenge of malicious botnets and other distributed cyber threats can only effectively be addressed by diverse solutions throughout the entire ecosystem, and USTelecom and its members readily accept the responsibility that ISPs have as an important part of the multilayered and distributed solutions to this challenge. ISPs' efforts in this area have been fundamental to our central role in the Internet and communications ecosystem for decades. However, the efforts of ISPs alone cannot sufficiently address the threats and vulnerabilities posed by botnets and other cyber threats. Rather, all stakeholders in the Internet and communications ecosystem must take bold new steps to prevent these threats in the first place.

The development of the Final Report offers the chance to begin to more specifically delineate and promote awareness throughout the ecosystem of the complex and interrelated legal, operational, technical, and financial elements of "shared responsibility." The fundamental handicap to addressing this challenge is the general lack of strategic and operational awareness between the components of the ecosystem regarding both the threats themselves and also the roles of the relevant players in addressing those threats. In order for the ecosystem to develop an "immune system" that can prepare for and respond to these threats as quickly as they develop and proliferate, stakeholders throughout the ecosystem must collectively be better poised for coordinated action than the malicious actors are. Given the dynamism of the threat, market-driven solutions are the best way to address these challenges.

Developing and deploying these solutions will require "collaboration by design" that accounts for the highly diverse and distributed complexity of the Internet and communications ecosystem. This intricate system is composed of disparate human and automated components throughout the private sector consumer and enterprise marketplace, academia, civil society, local governments and national governments worldwide. While there are some venues in which these entities meet, these efforts are disjointed and there is a need to better design and implement collaborative processes such that these disparate stakeholders are aware of their role and take action in response to cyber threats.

End-point devices are crucial to this challenge, and we strongly support concerted efforts in industry to promote NIST and NTIA stakeholder-driven consensus processes to improve device security, as recommended in Action 1.4. The same is true for software applications providers, which have a key role to play in the ecosystem and need to have a prominent seat at the table; likewise, we support recommended Action 1.2. Many other key stakeholders, including edge service providers, have not been involved in these policy discussions to this point and are not included in the Draft Report's recommendations; we urge the drafters of the Final Report to seek input from these players as well.

The draft report promotes the idea of shared responsibility, but, as we stated in our July 28 comments in response to the original request for proposal:

> "the various specific responsibilities of the components of the ecosystem remain unclear and, in most cases, altogether unknown. This creates a scenario that is ripe for the fallacy of utopian policy solutions narrowly focused on one or two components of the

> ecosystem – for instance, that ISPs can simply be empowered to shut down all botnets, or that devices can be universally secure, or that consumers can become omniscient."[2]

USTelecom therefore believes that the Final Report should call for a follow-up government-convened process led by NTIA, NIST, and DHS, with the support of other agencies as needed, to examine in depth the specific actions that each group of stakeholders (e.g., ISPs, device makers, software developers, enterprises etc.) should take, the means to promote those actions, obstacles to implementation, and policy levers that can be pulled to overcome those obstacles. In other words, what specifically are the concrete, actionable mechanisms through which stakeholders "share responsibility?"

B. DEVICE AND IOT PLATFORM SECURITY

As noted above, USTelecom praises, in particular, the draft recommendations regarding device security. Beyond the security of end-point devices, the Draft Report also reflects our view that government and industry should initiate further efforts to advance new gateway solutions provided by the dynamic market for network management devices and tools such as "smart routers," middleware, cloud-based IoT security solutions, and network isolation and filtering, and the developing standard for manufacturer usage descriptions (or MUDs). Network service providers are also investing in capabilities to secure IoT devices at the network layer. This is an evolving marketplace and we anticipate that more solutions will be brought to market in the future. We believe the Final Report should call for a follow-up government-convened process led by NTIA, NIST, and DHS, with the support of the FTC and other agencies as needed, to promote market awareness of such developing solutions.

[2] Comments of USTelecom, NTIA Docket No. 170602536-7536-01, July 28, 2017, at 13.

In particular, as the Draft Report notes in Action 3.3, large enterprises (including both private sector companies and government agencies) must boost the "demand side" of the market for security which will help drive the development of these solutions. And as noted in Action 3.1, device and platform suppliers must advance – and affirmatively market – the "supply side" of the market for security in order to clarify the benefits of secure devices and IoT platforms for individual consumers and small businesses. The government could play a role here by both promoting awareness of the security risks and the availability of solutions, without putting its thumb on the scale in favor of any particular solution given that the market for these solutions is nascent. Additionally, as the National Security Telecommunications Advisory Committee (NSTAC) Report to the President on Internet and Communications Resilience noted, we support efforts to focus on the security shortfalls of small, inexpensive, overseas-manufactured products (as distinct from products developed by large sophisticated manufacturers).

Finally, many other countries and jurisdictions are considering IoT device certification regimes and other requirements. We believe that the U.S. government should make a concerted effort internationally to align the various policy approaches so as to avoid duplicative and overlapping IoT device security requirements. To this end, we support the Draft Report's recommended Action 1.1 to develop Cybersecurity Framework profiles for IoT devices in various verticals (e.g., auto, healthcare, consumer etc.) that could be introduced as a model in international standards bodies like ISO to drive harmony in the approach.

C. INFRASTRUCTURE AND INTERNET SERVICE PROVIDERS

Two particular areas of interest for USTelecom regarding shared responsibility are (1) the "infrastructure" section, and (2) the recommendations regarding ISPs.

First, the draft report explicitly notes that “infrastructure” is not just ISPs, but its discussion regarding infrastructure focuses mostly on ISPs. The Final Report should begin to flesh out the developing contours and details of the Internet infrastructure, to include cloud providers, DNS providers, Web hosts, content delivery networks, networking equipment developers, and other stakeholders that may increasingly be considered part of the Internet infrastructure such as edge service providers. The follow-up government-convened process regarding “shared responsibility” that we recommend above will advance this crucial understanding of the players and responsibilities that comprise the Internet infrastructure.

Second, regarding ISPs in particular, the Draft Report properly observes that because automated, distributed attacks on the global Internet are an ecosystem-wide problem, the issue will require coordination on policy and governance solutions across sectors. The Draft Report states that:

> “while many solutions involve active coordination with ISPs, putting sole responsibility at the network level would make all traffic dependent on this connective layer to determine what ‘good’ traffic looks like, empowering ISPs to decide what fundamentally is and is not allowed on the Internet. Moreover, such ISP decision making would invariably both block traffic that in fact is ‘good’ and miss traffic that should be blocked.”[3]

USTelecom and its members strongly agree.

Therefore, in accordance with the recommendations of the NSTAC Report, we believe that the Final Report should call for a follow-up industry-led process facilitated by DHS as the

[3] Departments of Commerce and Homeland Security, Draft Report to the President, *Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats*, January 5, 2018, at 20.

Communications Sector's Sector Specific Agency, with the active support of NTIA, NIST, the FCC, DOJ and other agencies as needed, to work with the CSCC to assess and develop baseline actions (e.g., BCP38/84, security peering arrangements, port/site blocking, etc.) that could be undertaken by ISPs or network services providers to play their role in the ecosystem, determine to what extent these actions are being implemented today, obstacles to implementation, recommendations to enhance implementation, and the government and law enforcement support necessary to maximize effectiveness. This would include a particular focus on the challenges that face smaller ISPs with substantially more limited resources. We propose that this effort should result in a report developed by the CSCC jointly with DHS by the end of 2018.

The Communications Sector has previously pioneered landmark sector-wide initiatives along these lines, such as the effort in the Fourth Communications Security, Reliability and Interoperability Council (CSRIC) to implement the Cybersecurity Framework in the various segments of the Communications Sector – the most in-depth effort of any critical infrastructure sector to implement the Framework. Likewise, the action we propose here regarding ISPs' ecosystem activities would chart new ground in strategic and operational cybersecurity coordination; as with the previous effort regarding the Framework, this proposed CSCC-DHS effort would result in a detailed action plan for ISPs, government actors, and other stakeholders regarding implementation and engineering, managed services, service level agreements, peering and information sharing, botnet takedowns, and other issues.

We hope this effort will serve as a model for other critical infrastructure sectors and their Sector Specific Agencies and regulatory authorities.

D. INTERNATIONAL COORDINATION

We agree with the Draft Report's recognition for the need for international coordination, given its observation that distributed and automated cyber threats are a global problem that cannot be addressed solely with domestic U.S. solutions. Large multinational enterprises, allied governments, international standards organizations, and other stakeholders all have a role in improving coordination on these matters. As with information sharing, the Final Report should provide processes to determine what "international coordination" should mean more specifically. For instance, what is anticipated and expected at the implementation and engineering level? How can we further promote advanced international peering agreements that allow for streamlined international law enforcement takedowns and reduction in international bot-driven traffic from insecure devices? And what are the logistics anticipated to accomplish this? Also, as noted above, the need for harmonization internationally is becoming more and more critical in particular in the IoT space as the potential for duplicative, overlapping, uncoordinated regulations is large and it could stunt the growth of the IoT marketplace.

In all of these areas, the Final Report should provide concrete steps to move the needle in collaboration with international partners and across borders. The perspectives and engagement of private sector stakeholders, particularly ISPs, will be essential in this process, but the diplomatic aspects of these initiatives will require government leadership.

To this end, we believe that the Final Report should call for a follow-up government-convened process led by NTIA, NIST, and DHS, with the support of the DOS, the DOD and the DOJ, to develop a coordinated approach among allied governments and market economies such as the United Kingdom, the countries of NATO and the EU, and other key allies such as Japan and South Korea.

E. SMALL ISPS AND ENTERPRISES

USTelecom strongly believes that the government's fundamental and primary role must be to support the companies that are our country's front-line defenders against sophisticated criminal and nation-state adversaries. However, some of these defenders are small and mid-sized ISPs that have limited funds, narrow operating margins and market resources to play a leading role on the front lines. To sufficiently support small and mid-size ISPs, we recommend that the Final Report contain some common-sense solutions, such as specific forms of assistance and awareness campaigns targeted particularly at the markets these smaller ISPs serve. To this end, we believe that the action mentioned above with the CSCC and DHS to identify a baseline set of practices for communications must take into account the issues facing small ISPs and as part of identifying obstacles and potential remedies to those obstacles the industry should recommend actions that may increase deployment among small ISPs.

III. CONCLUSION: REGARDING NEXT STEPS, THE FINAL REPORT SHOULD CALL FOR CONCRETE ACTIONS TO EMPOWER PRIVATE SECTOR LEADERSHIP.

Again, we reiterate our support for the current government-facilitated private sector-driven process, and we recommend that the Final Report also call for organized private sector efforts to effectuate the recommendations and action items at the strategic and operational level. The initiatives we will announce in the coming weeks will provide a running start.

Over the longer term, as we noted in our July 28 comments, we recommend that to sustain this positive momentum, the government should invest in sufficient structural support for these private sectors efforts. There is a considerable disparity between the funding and personnel applied to government-only cyber activities as compared to the funding and personnel dedicated to industry-facing activities at the Department of Commerce (DOC), DHS and DOJ/the Federal

Bureau of Investigation. We recognize the importance of government cybersecurity capabilities, but the gross shortfall in investment in the parts of the government that support industry-driven cybersecurity processes and industry-government collaboration constitutes a long-term threat to our national security, as it creates a bottleneck for crucial industry input and solutions. As we have sought to make clear through our various recommendations described above, there remains considerable work to be done by the government stakeholders that are on the wrong side of this resource differential – and that work will span not only the time before the Final Report is due in May 2018, but, optimally, long after that. Given the stakes for our national security and economic competitiveness, the Administration should ensure that the DOC and DHS have the resources to pursue these recommendations and to address these important issues more generally. We therefore recommend that this long-term structural and budgetary imperative be included in the Final Report.

USTelecom and its members stand ready to participate actively – and, as appropriate, take the lead – in the follow-up initiatives we recommend above.