In the Matter of	**)**	
	)	
Promoting Stakeholder Action	**)**	
Against Botnets and Other	**)**	**NTIA Docket No. 170602536-7536-01**
Automated Threats	**)**	
	)	

Comments of Motorola Solutions, Inc

Introduction

Motorola Solutions, Inc (MSI) appreciates the opportunity to provide comments on the National Telecommunications and Information Administration's (NTIA) Request for Comments on "Promoting Stakeholder Action Against Botnets and Other Automated Threats". We hope the NTIA will find these comments helpful as it continues to assesses the security technology and policy landscape of the Internet of Things as it exists today, and evaluates what role the U.S. Government should play going forward in helping to mitigate the potential threat of botnet attacks.

There is no longer any doubt that the Internet of Things will provide the industrial world with new ways to enhance operations across manufacturing, energy, agriculture, transportation and other critical sectors of the economy. However, the scope of the threat posed by botnets that are assembled from inadequately secured IoT devices and then used to launch automated attacks on communication networks or industrial control systems cannot be exaggerated. We therefore applaud the NTIA for examining this issue, and working with all of the key stakeholders to identify ways to mitigate these risks.

What Industry Is Already Doing to Address These Threats

As MSI has previously noted[1] the Internet of Things faces a variety of challenges, some of them familiar, and some of them far different than those that we have faced before. For example, connecting physical objects to the internet and providing them with logical properties like control and monitoring introduces a whole new set of concerns and challenges that must be addressed and managed. If the security of these devices can be compromised, making them part of a botnet could pose risks over and above remote attacks over the network, to potentially include attacks that could damage life or property.

[1] Department of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, Comments of Motorola Solutions, Inc., June 2016, available at: https://www.ntia.doc.gov/files/ntia/publications/msi_iot_rfc_comments_060216.pdf

This RFC requests input on a series of broad questions, including what solutions are currently working to address automated and distributed threats, what gaps still exist in these remedies, and what role the government should play in addressing the threats posed by botnets and other automated threats. Below we provide some proposals to be considered in response to these questions.

Approaches That Are Working

We believe the public-private partnership (PPP) approach is the most effective way for government and industry, working together, to identify and address the complex security threats to the Internet of Things landscape, including the creation and manipulation of botnets. Rather than adopting a top-down regulatory approach, a more appropriate role for government will be to work with industry to help identify issues and threats, and then leverage its ability to bring stakeholders together to broadly address these issues. The NTIA multi-stakeholder process currently being used to address Internet of Things security issues is a good example of the government using its convening power to achieve consensus across the industry to address a common set of problems. This approach will ensure buy-in from the stakeholders, and give them the incentive to invest in the identified solutions to address their own unique security risks.

In 2015 The FCC TAC Cybersecurity WG released a White Paper[2] detailing its assessment and recommendations for addressing security and protection of IoT consumer products. This White Paper identified gaps in cybersecurity for existing IoT solutions, noted a variety of industry standards that had been or were being developed to address the IoT cybersecurity landscape, and listed multiple best practices that have already been developed for securing IoT devices. This effort provided some important recommendations for improving security of consumer IoT devices, and also provided an important example of how the Public-Private Partnership approach can achieve industry consensus on identifying and mitigating cybersecurity threats in the IoT space.

Any effort to address botnets and other automated threats should also leverage, where possible, consensus-based industry standards. The information and communications technology industry (ICT) already embraces numerous standards and best practices for assessing and managing risk, at both the operational and technical level. Open, voluntary standards development efforts led by industry will ensure that these standards-based solutions will be interoperable and applicable across a wide array of market-segments, use cases and geographies. The use of international standards and best practices, rather than market-specific or country-specific standards, will also help encourage a global approach to addressing these issues, which pose a threat that is global in scope.

[2] Federal Communications Commission, Technological Advisory Council, Cybersecurity Working Group, Applying Security to Consumer IoT Devices Subcommittee, Technical Considerations White Paper, December 2015, available at https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf

What is Still Needed

With all of the effort already underway to assess botnet threats, there are still policy gaps that need to be addressed. There are many opinions regarding the best approach for crafting an overall policy for addressing this sort of automated threat, with some arguing for a common policy approach, to leverage knowledge gained across the IOT landscape. While it does make sense to begin with a common horizontal policy framework where possible, mitigation of the threats posed by botnets and other automated attacks would also benefit from a more detailed categorization of the IOT landscape. IOT categorization is critical because different IOT applications will have different levels of vulnerability, and therefore some could sustain a greater impact if attacked. Cybersecurity attacks on IoT systems such as transportation, utilities or industrial systems can differ from regular cybersecurity attacks, since these attacks can affect physical objects like the electrical grid, safety-related networks or other potentially life-impacting devices or networks.

Therefore, we recommend starting with a horizontal policy framework that takes into account the input of agencies and stakeholders with a wide variety of perspectives to maximize the value of the resultant solutions for addressing botnet threats. From that platform, those recommendations and solutions can then be enhanced, as needed, based on the sometimes unique needs of the different IOT market segments. This customized approach to botnet resilience policy could provide more benefit than simply taking a one-size-fits-all approach.

Governance, and the Role of the Government

While the government has a key role to play in the mitigation of botnet threats, it should seek to avoid taking a heavy-handed regulatory approach that cannot keep pace with technology innovation, or the evolution of IOT-based cybersecurity threats. The rate at which the risks posed by botnets are evolving is accelerating, and the identification and development of responses to these threats must be just as nimble. Leveraging the public-private partnership approach as discussed above will provide industry and the government with the most up-to-date information and solutions to these threats. In its IoT Green Paper, issued by the Department of Commerce earlier this year, one commenter argued that “overly prescriptive regulations could impede stakeholders’ abilities to respond to ever-changing threats…”[3], and we agree that this is a valid concern. Foregoing rigid and burdensome regulations will avoid a regulatory environment that could actually impede the development of innovative solutions to the risks posed by botnets. Where regulation is necessary, the government should adopt an approach that is transparent and flexible enough to avoid impeding the development of effective solutions on a global scale, always keeping in mind that regulations can impose added cost and delays in getting solutions into the marketplace.

[3] Department of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, Fostering the Advancement of the Internet of Things, January 2017,at 25, available at https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

Any policies and regulations that are ultimately adopted to address botnet threats should always avoid favoring one technology over another. These policies should remain technology-neutral to avoid undermining competition or eliminating emerging innovative solutions that might appear after the policies have been adopted. Government policies should assess the relevant risks to the stakeholders and the benefit to be gleaned from compliant solutions, and then encourage market innovators to develop solutions that are optimized to address these quickly evolving threats.

To advance the knowledge and capabilities of industry in combating these threats, the government can provide much-needed assistance by funding research, education and industry-led standards development directed at defending against automated threats. By providing funding for research into cybersecurity vulnerabilities and botnet construction/operation, the government could help advance the identification and deployment of leading-edge industry solutions targeted at mitigating botnet risks. Making funding available for understanding the risks, and encouraging the use of industry-identified best practices for mitigating botnet risks, could greatly improved the national, and even global, responses to botnet attacks. In addition, small and medium-sized businesses (SMBs) who generally tend to be less aware of, or sensitive to, the risks posed by botnets could greatly benefit from an expanded government effort to educate them on cybersecurity threats, and the risks to their enterprises.

Finally, government support for the development of industry-led standards for assessing and mitigating the threats posed by botnets could help increase the market buy-in and support for the development of the necessary standards. Due to the critical nature of many of these systems, the Federal government could also enforce, and in some cases finance, the usage of cybersecurity protections in critical infrastructure & safety related automated systems.

Conclusion

Motorola Solutions thanks the NTIA for this opportunity to provide inputs on the Request for Comments on “Promoting Stakeholder Action Against Botnets and Other Automated Threats.” As noted above, we believe the U.S. Government has an important role to play in bringing together all of the key industry stakeholders. By doing so, it can help to advance the technologies and solutions for mitigating botnet risk without taking a burdensome regulatory approach to cybersecurity requirements and solutions for the Internet of Things.