February 12, 2018

VIA EMAIL: *counter_botnet@ list.commerce.gov*

National Telecommunications and Information Administration
U.S. Department of Commerce
Attention: Evelyn L. Remaley
Deputy Associate Administrator
1401 Constitution Ave. NW, Room 4725
Washington, DC 20230

Re: IT SCC Comment on Draft Report to the President on Promoting Stakeholder Action Against Botnets and Other Automated Threats

The Information Technology Sector Coordinating Council (IT SCC) welcomes the opportunity to respond to the Draft Report to the President on Enhancing the Resilience of the Internet and Communications Technology (ICT) Ecosystem Against Botnets and Other Automated, Distributed Threats (Report).

Under the National Infrastructure Protection Plan, the IT SCC serves as the principal IT Sector organization for developing, coordinating and implementing with the Department of Homeland Security (DHS) and other U.S. government stakeholders, consensus based policy issues on a wide range of cybersecurity and critical infrastructure protection activities.

The IT SCC agrees that botnets and other automated, distributed threats constitute business, security and privacy risks to critical infrastructure, industry, governments and consumers. We welcome the government's interest in developing goals and action items to address these threats, and we are enthusiastic about working with our government partners to address this significant challenge.

Our submission focuses on the following principles:

1. The Federal Government should leverage public private partnerships in developing and implementing recommendations and action items;
2. The Federal Government, when possible, should utilize existing work streams, developed in partnership with industry stakeholders, in implementing these recommendations;
3. The Federal Government should prioritize coordination amongst the multiple government and industry stakeholders to implement the action items under this Report.

Leveraging Public Private Partnerships

The IT SCC recommends that the Federal Government work closely with industry and other stakeholders, through public private partnerships, to further prioritize, develop, coordinate, and implement the action items under this draft Report.

Public private partnerships, and stakeholder driven processes remain the most effective means of developing sound, consensus based practices and approaches.

Stakeholder engagement ensures that different security and technology perspectives and experiences are weighed in policy development, and it encourages greater participation and buy-in when policies go into effect. In addition, such engagement enables industry and government to better understand the perspective and needs of the other. Through this understanding, public-private engagements enable the community to drive to consensus, and an outcome that is supported by both industry and government. Finally, effective public private partnerships can help promote security while allowing for technology innovation and development.

The Federal Government should work closely with the IT SCC, the Communications SCC, and other key stakeholders in the further development and prioritization of recommendations and action items under this Report, in particular those that impact private industry. To demonstrate the benefits of industry government collaboration, we note the continued value provided by the IT Sector Baseline Risk Assessment. This document was developed by subject matter experts from industry and government, and represented a new approach to sector-wide risk assessment and risk management. The methodology in this approach continues to be used within the IT Sector and has been leveraged by other sectors as well. Similarly, the IT and Communications sectors collaborate regularly on policy and operational issues.

The development of the Framework for Improving Critical Infrastructure Cybersecurity (Framework) represents another excellent example of leveraging stakeholder input to develop effective outcomes through a public private partnership. The IT SCC has been an active contributor to the Framework development and update process. We agree with the Report's finding that a foundational step towards the vision of secure enterprise networks would be widespread enterprise application of the Framework.

Utilizing Existing Work Streams

There are currently multiple work streams involving public private partnerships to address security risks emanating from IoT devices and infrastructure. The IT SCC believes the Federal Government should utilize these existing work streams and ensure that any future guidance or recommendations are in alignment with these efforts.

For instance, Action item 2.3 states that the Federal Government should lead by example and demonstrate practicality of technologies, creating market incentives for early adopters. Under this action item, the Report recommends that the Federal Government establish procurement regulations that favor or require commercial-off-the-shelf software developed using secure development tools and processes.

The IT SCC has established a joint working group with the Department of Homeland Security, using the partnership model, to develop cybersecurity procurement guidance for federal officials in the acquisition of IoT products and services. This work stream has active involvement from multiple industry stakeholders and includes representatives from a broad range of federal agencies.

The goal for the project is to focus on a subset of IoT implementations – those most prevalent in the Federal environment – and to identify baseline security considerations applicable to acquisitions. The guidance will include an overview of IoT cybersecurity considerations, a procurement lifecycle mapping, and additional considerations for implementation, among other key security issue areas.

Coordination and Prioritization

While cybersecurity is now acknowledged as a critical priority by government and industry stakeholders alike, the near universal recognition of the problem is spurring often divergent initiatives from policymakers across the USG (as well as at the state and local government level). Unfortunately, these well-intentioned policymaking efforts to address cybersecurity challenges are often uncoordinated, raising the specter of not only siloed but often prescriptive regulatory proposals, and are also increasingly calling for the premature development and implementation of cybersecurity measures or metrics that favor compliance-based cybersecurity models and are disconnected from any clear cybersecurity benefit.

In the same way, this topic has received a lot of attention among policymakers outside of the United States. These policymakers are similarly developing their own policies. To the extent possible, the United States should coordinate botnet mitigation strategies directly with other countries as well as through existing forums for international collaboration and policy development.

Among small businesses and home users, the threat of botnets barely registers. For this segment of stakeholders, education and awareness is still paramount. Until they understand the prevalence and impact, as it relates to *their* business, they will not take action or buy more secure versions of the same IoT product. It is important to respect where each stakeholder segment lies on the continuum of ignorance, awareness, and action. While large businesses are aware and need help reacting, small businesses need to at least be shepherded into awareness before they can even begin to comment on regulatory impact.

A primary role the government should take in coordinating effort is to make threat data transparent. Neighborhood crime statistics and national school rankings are examples of government created data that helps individuals make better choices when investing in their home and family. Likewise, State Department travel advisories help US citizens make decisions when traveling abroad. Sector and industry based reporting on incident rates and impact studies exposes risk and facilitates deliberate decision making. Extending reports and research globally is of equal value. Even the smallest of businesses can interact on a global scale, and knowing what hotspots to avoid in business dealings is invaluable information.

Successful implementation of the Report's action items will require dedicated coordination of efforts and prioritization. Implementation should seek to avoid overlap to the extent possible and must avoid conflicting guidance. Further, given the broad range of action items, it will be important for the government to work with industry stakeholders to prioritize action items with respect to both timelines and impact. The IT SCC can help work with DHS to prioritize efforts.

Conclusion

The IT SCC looks forward to working with its government partners and industry and other stakeholders to address the challenges posed by botnets and other automated threats. We believe a dedicated commitment to utilizing the public private partnership model will yield the strongest outcomes. Further, we recommend that the government leverage existing partnership work streams in implementing the Report's recommendations. And, we believe that coordination and prioritization of the range of stakeholders and work streams will be necessary for success. We thank you for the opportunity to provide comments and look forward to continuing our partnership with the Federal Government to improve our nation's cyber defenses.