To: US Commerce Department and Homeland Security Department
Sent via email to: Counter_Botnet@list.commerce.gov

On behalf of Financial Services Information Sharing and Analysis Center (FS-ISAC), I am commenting on "Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats", which the Administration prepared in response to Executive Order 13800 issued on May 11, 2017.

FS-ISAC is a non-profit corporation that was established in 1999 and is funded by its member firms. With about 7,000 members worldwide, FSISAC is a member-driven organization whose mission is to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the global economy. FS-ISAC shares threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid response communications for both cyber and physical events; conducts education and training programs; and fosters collaborations with and among other key sectors and government agencies.

We applaud the Administration for focusing on this important topic given that the financial services sector is dependent on the telecommunications sector and has worked in collaboration with telecommunications companies (and US Government agencies) for many years to respond to and mitigate risks from cyber-attacks targeting the telecommunications and financial services sector. This collaboration is focused on protecting both critical infrastructure and customers.

Financial Sector Collaboration Should be Highlighted in the Report

In light of these collaboration efforts we would like to request that the final paper reflect some of this collaboration. Specifically, we request the final paper include references to the following:

- On page 5, we suggest adding that the financial services sector (via a joint effort by FS-ISAC and BITS/Financial Services Roundtable in 2013) engaged the major Internet Service Providers (ISPs) in a series of discussions to review the impact of cyber-attacks (e.g., distributed denial of service attacks, growth of botnets, malware) and potential collaborative strategies the financial sector and the ISP sector could undertake to mitigate the risk of cyber-attacks. This collaboration was in response to the distributed denial of service attacks in 2012 and 2013 when an organization, backed by a foreign country, targeted dozens of financial institutions. The attacks were disruptive; but they also resulted in unprecedented levels of information sharing among financial institutions and the US government and resulted in greater collaboration with the telecommunications sector. For example, information sharing proved to be extremely beneficial to firms that were targeted on the second, third and fourth wave of DDoS attacks given that the lessons learned from firms on the first wave were rapidly shared with others that had yet to be attacked. The DDoS attacks also led to increased collaboration with the major ISPs with financial institutions, facilitated by the FS-ISAC and BITS/Financial Services Roundtable.
    - In addition, the financial services sector collaborations including Industry Botnet Group's clean data center initiative (a voluntary mechanism to identify the bot or botnet), Cloud Security Alliance's anti-bot working group, and the Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Council (CSRIC) working group on botnet mitigation and efforts to explore potential legislative initiatives to limit liability and address net neutrality concerns.
    - Furthermore, the FS-ISAC participates in the National Council of ISACs and is also a founding member of the Global Resilience Federation, both of which are designed to promote cross sector sharing, including with the Communications ISAC. Cross sector sharing is an important cyber measure that can contribute to initiatives such as the 'clean pipes' type initiative undertaken by many service providers.
- On page 8, we suggest adding information on financial services sector efforts with Microsoft and other companies to take legal action against botnets. For example, FS-ISAC has partnered with technology companies including Microsoft, Agari and others including American Bankers Association (ABA) and NACHA on past botnet takedowns, including SpyEye, Zeus and Citadel botnets and malware-serving sites.
- On page 12, we suggest mentioning FS-ISAC efforts to share information in response to the September 2016 attacks leveraging compromised "Internet of Things" (IoT) devices (e.g., DVRs and digital cameras) that resulted in some of the largest DDoS attacks in recorded history.

Comments on Goals

We also have a few comments on the goals which start on page 23 of the draft paper. Overall, we believe the goals are too general and lack clear accountability in terms of which US Government agencies will take the lead on these efforts and how various private sector participants will be held accountable.

On page 30, the paper recommends that industry and government should collaborate with the full range of stakeholders to continue to enhance and standardize information-sharing protocols (action 2.4). We strongly agree with this recommendation and we also recommend that the paper emphasize that companies should share information and analysis with each other and in collaboration with US government resources.

The report does not adequately discuss the importance of software development and security awareness and training. From a security perspective, software developers who develop the code for an application need to adopt a wide array of secure coding techniques. Most developers do not learn secure coding practices and the frameworks they use often lack critical core controls that are not secure by default. The developers should follow the software development security checklist which enlists the controls in order of priority, starting from the most important control, including:

- Verify for security early and often
- Parameterize queries
- Encode data
- Validate all inputs
- Implement identity and authentication controls
- Implement appropriate access controls
- Protect data
- Implement logging and intrusion detection
- Leverage security frameworks and libraries
- Error and exception handling

In order to emphasize the importance of secure coding, we recommend that the report encourage secure coding practices in schools so that developers and designers of IT products and services use design principles that build security into new products and services that focuses on security and attack resilience as well as performance and functionality. Security would be an integral part of the initial designs for future secure and attack-resilient computer architectures, and it would be integrated into every aspect of the hardware and software design life cycles and research agendas. Designers and developers would emphasize defensive design and implementation with the expectation that systems will have to deal with user mistakes and malicious adversaries. End users should be aware of security matters and diligent in their efforts to promote security.

We applaud the report's focus on education and awareness given that this is an important building block for enhancing security and resiliency. Simple steps like educating users to secure their IOT devices by changing their default passwords can go a long way to prevent these botnets to grow to such large numbers.

We believe the recommendation for the federal government to lead by example and demonstrate practicality of technologies, creating market incentives for early adopters (Action 2.3) is important. Products should be secured during all stages of lifecycle and the federal government can play an important role in purchasing products and services that adhere to higher security and resiliency standards. The federal government can also help in promoting reliable security ratings of products so that companies and individuals have better knowledge in evaluating products and services.

Thank you for the opportunity to comment on the draft report.

Sincerely,

John W. Carlson
Chief of Staff, FS-ISAC