July 28, 2017

National Telecommunications and
Information Administration, U.S.
Department of Commerce,
1401 Constitution Avenue NW
Washington, DC 20230

To Whom It May Concern:

On behalf of our members, the Edison Electric Institute ("EEI") is pleased to submit this response as part of the request for comment on "Promoting Stakeholder Action Against Botnets and Other Automated Threats," which the National Telecommunications and Information Administration ("NTIA") published in the Federal Register on Tuesday, June 8, 2017.

EEI is the association that represents all U.S. investor-owned electric utilities and its affiliates worldwide. Our members provide electricity for 220 million Americans and operate in all 50 states and the District of Columbia, accounting for approximately 70% of the U.S. electric power industry. Protecting the nation's electric grid and ensuring a safe and reliable supply of power is the electric power industry's top priority. Thus, managing cybersecurity risk is a top priority.

We support the Federal government's efforts to address the threats to critical infrastructure perpetuated by automated distributed attacks, as directed by the President's Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." We appreciate the opportunity to provide comments on possible actions that can be taken to address these threats to the digital ecosystem.

Electric industry experts have identified machine-to-machine cyber attacks as one of the top threats to electric infrastructure. As electric infrastructure becomes increasingly interconnected and automated with the deployment of smarter technologies, the likelihood of a converged information technology/operational technology (IT/OT) cyber attack increases, and could cause power outages, costly damage to infrastructure, or other consequences to the life, health, and safety of Americans. The December 2015 Ukraine attack, the first publicly-acknowledged incident to result in power outages through cyber means, initially compromised the corporate network and ultimately corrupted SCADA operations. IT/OT attacks highlight the importance of securing and segmenting both IT and OT environments (and the links between them) to mitigate potential impacts to energy grid reliability stemming from a sophisticated cyber intrusion. By continually assessing and identifying ways to address these risks, companies are reducing the disruptive conditions associated with these top threats, thus strengthening the overall resilience of the electric grid.

In the published request for comment, the NTIA requested responses to the following questions:

1. **What works**: What approaches (e.g., laws, policies, standards, practices, technologies) work well for dealing with automated and distributed threats today? What mechanisms for cooperation with other organizations, either before or during an event, are already occurring?
    - A baseline for asset configuration that incorporates security best practices for Internet-connected devices should be established. Securing endpoint devices will reduce the overall number of devices from which a botnet can draw on to direct malicious traffic. Common defenses for botnet attacks include traffic filtering, bandwidth increases, and/or Domain Name Server ("DNS") modification.
    - Vendor solutions exist that allow companies to monitor their own Internet traffic and that of their suppliers. These tools allow companies to monitor certain aspects of supply chain risk, including the threat of automated distributed attacks.
    - Other tools in the market, such as two-factor authentication and detecting machine versus human interaction help reduce certain botnets.

2. **Gaps**: What are the gaps in the existing approaches to dealing with automated and distributed threats? What no longer works? What are the impediments to closing those gaps? What are the obstacles to collaboration across the ecosystems?
    - No common or baseline security standards exist for home-based Internet connected devices. There does not appear to be any minimum security requirements for these devices.
    - The drawback of emphasizing asset and configuration best practices is that often the assets in a botnet are not owned by private corporations. Rather, private individuals are responsible for ensuring that all of their devices are configured properly.
    - Automated distributed attacks leverage devices not owned by the victim of the attack. Device owners may not experience reduced functionality of the device used during the attack, making it difficult to incentivize good security practices.
    - The volume of DDoS attacks is increasing exponentially over time[1], making it much more challenging and expensive to remediate.
    - Organizations may be hesitant to share information about ongoing attacks against their organization with their respective Information Sharing and Analysis Centers (ISACs).
    - Countries where botnet attacks originate typically have more relaxed laws relating to cybercrime and as a result have become havens for these types of activities. Attribution of these attacks is often difficult, and international cooperation will be required to address this issue.

3. **Addressing the problem**: What laws, policies, standards, practices, technologies, and other investments will have a tangible impact on reducing risks and harms of botnets? What tangible steps to reduce risks and harms of botnets can be taken in the near term? What emerging or long term approaches may be promising with more attention, research, and investment? What are the public policy implications of the various approaches? How might these be managed, balanced, or minimized?
    - Implementing secure asset configurations can significantly help to reduce botnet attack capacity. Specifically, securely configuring Internet of Things ("IoT") devices and

[1] https://www.dhs.gov/sites/default/files/publications/FactSheet%20DDoSD%20FINAL%20508%20OCC%20Cleared.pdf

assets running services vulnerable to DDoS amplification would significantly decrease current botnet capacities.

- Requiring users to change device passwords and adhere to current complexity criteria recommended by the Federal government prior to connecting devices to the Internet could reduce botnet capacity.
- Alignment with standards such as the Manufacturer Usage Description ("MUD"), which is under review with the Internet Engineering Task Force ("IETF"), could help mitigate or prevent distributed automated attacks by blocking improper communications by IoT devices and preventing lateral movement by attackers across different device types.
- Encouraging victims of botnet attacks to communicate with their ISACs and relay technical indicators and attack volume as they occur could help mitigate the overall impact of the attack.
- Study regulatory impediments and recommend solutions to increase reporting to the ISACs.
- Educate end users on placing IoT devices on a separate segmented network connection behind a firewall.
- The development of certification program with consumer rebates similar to EPA's "Energy Star," based on an engineering standard for IoT products, could help improve the baseline level of security for IoT devices.
- Develop incentives that encourage vendors to develop cyber threat mitigating products, and/or encourage companies to improve cyber security practices. Tax incentives for using best practice defenses are a possibility.

4. **Governance and collaboration**: What stakeholders should be involved in developing and executing policies, standards, practices, and technologies? What roles should they play? How can stakeholders collaborate across roles and sectors, and what should this collaboration look like, in practical terms?
    - Working groups including representatives from the public and private sectors should be included in the broader conversation about techniques to minimize the threat associated with botnets. Having open forums for sharing recent issues and best practices across sectors, including academia and cybersecurity professionals, will help identify cross-cutting solutions.
    - Local, state, Federal, and international law enforcement should coordinate the dismantling of botnets. State and Federal standards and policies must be aligned to avoid conflicting efforts.

5. **Policy and the role of government**: What specific roles should the Federal government play? What incentives or other public policies can drive change?
    - The Federal government, and in particular the Federal Bureau of Investigation ("FBI"), should continue to play a key role in the dismantling of botnets.
    - Incentives should be provided to encourage IoT devices to be securely configured by default.
    - Alignment with the MUD standard (or other similar standards) may help address issues related to automated distributed threats.

6. **International**: How does the inherently global nature of the Internet and the digital supply chain affect how we should approach this problem? How can solutions explicitly address the international aspects of this issue?
    - International bodies could use the classification of certain products and services under the International Treaty for Arms Regulation[2] or the Arms Trade Treaty[3] as a guide for monitoring the import and export of certain types of IoT devices due to their use as cyber weapons.
    - Another approach could be to follow Federal recall laws and regulations that require certain equipment, such as railcars, to meet public safety standards. Regarding IoT devices, this would require manufacturers to publicly disclose if their devices failed to meet certain cybersecurity standards and were compromised in an automated distributed attack. Disclosure time periods should be standardized to include both vulnerability identification, as well as sufficient time for remediation, either via firmware upgrade, or hardware replacement by the manufacturer.

7. **Users**: What can be done to educate and empower users and decision-makers, including enterprises and end consumers?
    - General security awareness for end users, such as placing IoT devices behind a firewall instead of directly connecting them to the Internet, could help reduce the number of attacking devices. A notification process for owners of devices utilized in an automated distributed attack would also help educate end users on device security.

On behalf of EEI's members, thank you for the opportunity to provide input to these important questions and to inform policies that can help secure critical infrastructure from cyber attacks.

Sincerely,

Scott I. Aaronson
Executive Director, Security & Business Continuity
Edison Electric Institute

[2] https://www.pmddtc.state.gov/regulations_laws/itar.html
[3] https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2013/06/English7.pdf