Response to Senator Warner's Letter
concerning Distributed Denial of Service Attacks

The following information addresses the questions in your letter.

1. ***What types of network management practices are available for internet service providers to respond to DDoS threats?***

Based upon the recent increase in significant DDoS attacks, the National Cybersecurity and Communications Integration Center (NCCIC) has published several alerts and bulletins outlining mitigation approaches and network management practices. On October 17, 2016, US-CERT released an alert, "Heightened DDoS Threat Posed by Mirai and Other Botnets."[1] This alert focuses on steps that users, administrators, and developers of Internet of Things (IoT) devices can take to implement improved security and quickly address a potential compromise that could result in the device being used in a DDoS. Example of fundamental steps to secure IoT devices include ensuring all default passwords are changed to strong passwords, updating IoT devices with security patches as soon as patches become available, and disabling Universal Plug and Play (UPnP) on routers unless absolutely necessary. The NCCIC has also published a "DDoS Quick Guide" with recommendations for general DDoS mitigations and an alert focused on UDP-Based Amplification attacks. To this point, the NCCIC has not produced an alert focused specifically on Internet Service Providers. Some network management methods, such as "blackholing" to block all traffic to a target website or "upstream filtering" may be untenable for targeted and massive DDoS attacks. As an alternative, ISPs may choose to use a cloud-based mitigation service that could route malicious traffic into a "scrubbing" server or provide customers with an alternate IP address for their Domain Name Service (DNS) query.

2. ***Would it be a reasonable network management practice for ISPs to designate insecure network devices as "insecure" and thereby deny them connections to their networks, including by refraining from assigning devices IP addresses? Would such practices require refactoring of router software, and if so, does this complicate the feasibility of such an approach?***

The Department of Homeland Security does not presently have a policy position on whether ISPs could designate insecure network devices as "harmful" in accordance with the FCC's Open Internet Rules and other relevant law and policy.

3. ***What advisories to, or direct engagement with, retailers of IoT devices have you engaged in to alert them of the risks of certain devices they sell? Going forward,***

[1] https://www.us-cert.gov/ncas/alerts/TA16-288A

what attributes would help inform your determination that a particular device poses a risk warranting notice to retailers or consumers?

The NCCIC, in particular through the Industrial Control System Cyber Emergency Response Team (ICS-CERT), has issued numerous advisories on potential cybersecurity vulnerabilities in certain devices. For example, the NCCIC has issued alerts about vulnerabilities in electric power meters[2], programmable logic controllers[3], and medical devices[4]. The NCCIC learns about such vulnerabilities from vendors, private researchers, and government partners. Critically, the NCCIC promulgates norms of responsible disclosure under which a vulnerability should only be disclosed when a viable mitigation is available and tested.

4. ***What strategies would you pursue to take devices deemed harmful to the network out of the stream of commerce? Are there remediation procedures vendors can take, such as patching? What strategy would you pursue to deactivate or recall the embedded base of consumer devices?***

On November 15th, DHS published *Strategic Principles for Securing the IoT*. This document promulgates non-binding strategic principles designed to enhance security of the IoT across a range of design, manufacturing, and deployment activities, and includes relevant suggested practices for implementation. It is a first step to motivate and frame conversations about positive measures for IoT security among IoT developers, manufacturers, service providers, and the users who purchase and deploy the devices, services and systems. In particular, the document recommends that IoT developers, vendors, and users:

- **Incorporate Security at the Design Phase**: Security should be evaluated as an integral component of any network-connected device. While there are notable exceptions, economic drivers motivate businesses to push devices to market with little regard for security.
- **Promote Security Updates and Vulnerability Management**: Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies.
- **Build on Recognized Security Practices**: Many tested practices used in traditional IT and network security can be used as a starting point for IoT security. These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices.
- **Prioritize Security Measures According to Potential Impact**: Risk models differ substantially across the IoT ecosystem, as do the consequences of security

[2] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-16-263-01
[3] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-15-224-02
[4] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01

failures. Focusing on the potential consequences of disruption, breach, or malicious activity is critical for determining where in the IoT ecosystem particular security efforts should be directed.

- **Promote Transparency across IoT**: Where possible, developers and manufacturers need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Increased awareness can help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies.
- **Connect Carefully and Deliberately:** IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption.

5. ***Has the National Cybersecurity and Communications Integration Center (NCCIC) been in communication with the Federal Communications Commission, or other federal agencies, regarding these incidents?***

Since the recent DDoS incidents, the Department's NCCIC has engaged with federal incident response agencies, including the Federal Bureau of Investigation, the other federal cyber centers, and members of the intelligence community to understand the risk environment and identify viable mitigations. Strategically, DHS executes its role as the Sector Specific Agency for the Communications Sector in part through close collaboration with the FCC's Public Safety and Homeland Security Bureau and the Communications, Security, Reliability, and Interoperability Council (CSRIC).

6. ***Does NCCIC have any recommendations for agencies charged with safeguarding consumer networks and data security?***

As noted, DHS recently published *Strategic Principles for Securing the IoT* as a first step in providing guidance to IoT developers, vendors, and users. The NCCIC is fully engaged in a whole-of-government effort to promote the security of consumer information and devices and will continue to work towards consensus recommendations that reflect input from government, the private sector, and academia.

7. ***What consumer advisories have you issued to alert consumers to the risks of particular devices?***

As noted in Question 3, the NCCIC has issued several alerts to notify the cybersecurity community about vulnerabilities in commercial devices. Of note, however, the NCCIC provides technical alerts intended for information security professionals. DHS works closely with consumer protection agencies such as the Federal Trade Commission and the Consumer Product Safety Commission to ensure that relevant cybersecurity information is promulgated to the general public.

8. ***Numerous reports have indicated that users often fail to install relevant updates, despite their availability. To the extent that certain device security capabilities can be improved with software or firmware updates, how will you ensure that these updates are implemented?***

DHS does not have statutory authority to mandate cybersecurity activities beyond the Federal civilian executive branch. Therefore, the NCCIC takes a voluntary approach to ensure that vendors and developers are aware of cybersecurity vulnerabilities and their relative importance. Such updates are provided through the US-CERT website and through standing distribution lists, web portals, and other convening mechanisms.

9. ***Do consumers have meaningful ability to distinguish between products based on their security features? Are formal, or third-party, metrics needed to establish a baseline for consumers to evaluate products? If so, has your agency taken steps to create or urge the creation of such a baseline?***

The NCCIC recognizes the current gap in cybersecurity metrics and is closely engaged with other agencies, the private sector, and academia to identify best practices in quantifying relative security. In particularly, the NCCIC provides input to and coordinates with private sector organizations such as Underwriters Laboratories in establishing a common baseline for consumer products. Moving forward, documents such *Strategic Principles for Securing the IoT* will help advance broad acceptance of a common baseline and, iteratively, a standard of due care.

10. ***Should manufacturers have to abide by minimum technical security standards? Has your agency discussed the possibility of establishing meaningful security standards with the National Institute of Standards and Technology?***

The Department's publication of *Strategic Principles for Securing the IoT* reflects a non-binding approach to baseline security standards. The NCCIC is engaged with the National Institute of Standards and Technology, the Federal Trade Commission, the Department of Transportation, the Food and Drug Administration, and other agencies to help inform the development of any future regulations and promote cross-sector alignment to a common standard.

11. ***What is the feasibility, including in terms of additional costs to manufacturers, of device security testing and certification, akin to current equipment testing and certification of technical standards conducted by the Federal Communications Commission under 47 CFR Part 2?***

The Department respectfully defers to the Federal Communications Commission in response to this question.