MICHAEL T. McCAUL, TEXAS
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Fourteenth Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

October 25, 2016

The Honorable Jeh C. Johnson
Secretary
Department of Homeland Security
Washington, DC 20528

Dear Secretary Johnson:

As you know, on Friday, October 21, hackers carried out successive, highly sophisticated cyber attacks against Dynamic Network Services, Incorporated's (Dyn) Managed Domain Name Servers (DNS) infrastructure.[1] These distributed denial of service (DDoS) attacks, carried out against each of Dyn's 18 data centers throughout the world at different times, resulted in significant disruptions for tens of millions of Internet Protocol (IP) addresses, outages for millions of brand-name Internet services such as Twitter, Amazon, Spotify, and Netflix, and estimated lost revenue and sales of up to $110 million.[2] While DDoS attacks are not uncommon, these attacks were unprecedented not only insofar as they appear to have been executed through malware that exploiting tens of thousands of Internet of Things (IoT) devices but also because they were carried out against a firm that is provides services that, by all accounts, are essential to the operation of the internet.[3]

These attacks, which are the subject of investigations by the Department of Homeland Security (Department) and the Federal Bureau of Investigation, bring into focus the importance of the Federal government and the private sector forging robust channels for information sharing. The Department, as the lead Federal department for the protection of critical infrastructure and the furthering of cybersecurity, has set as one of its primary strategic goals, to identify and understand interdependencies and cascading impacts among critical systems.[4] The attacks on Dyn underscore the interdependencies among operators in the Information Technology Sector. It is critical that the Department has a dynamic picture of these relationships and foster robust

---

[1] Statement of Kyle York, Chief Strategy Officer, Dynamic Network Services, Incorporated. http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/ (October 22, 2016).
[2] Id.
[3] "Unprecedented cyberattack involved tens of millions of IP addresses" Sara Ashley O'Brien. CNN. http://money.cnn.com/2016/10/22/technology/dyn-cyberattack/index.html. October 22, 2016.
[4] Department of Homeland Security's Annual Report for Fiscal Years 2015-2017.

relationships with those firms that are essential to the operation of the internet. As such, I would like to know how the Department's knowledge of such interdependences impacts its outreach and information sharing efforts and the status of its efforts to ensure that mechanisms are in place for companies providing essential services such as Managed DNS providers to access information and technical assistance from the Department.

Therefore, please provide the answers to the following questions by November 14, 2016:

1) According to the National Cybersecurity and Communications Integration Center (NCCIC) it became aware of the first DDoS attack through open source media reports two and half hours after the attack began.[5]
    a. Is it common for this situational awareness center to rely on media accounts to identify such far-reaching cyber attacks? If so, why?
    b. To what extent does the NCCIC receive information directly from industry groups, companies, and Information Sharing Analysis Organizations?
    c. As of 9:30am, NCCIC considered the incident closed; however, two attacks later ensued. What factors does the NCCIC use to declare an incident closed?

2) As you know, the Cyber Information Sharing and Collaboration Program (CISCP) is a no-cost information-sharing partnership between enterprises and DHS that is intended to share situational awareness across critical infrastructure communities, enhance cybersecurity collaboration between DHS and critical infrastructure owners and operators, and leverage government and industry subject matter expertise to collaboratively respond to cybersecurity incidents. Please provide information on the extent to which members of the Information Technology Sector are engaged with DHS through CISCP. Additionally, how many DNS providers, cloud providers, and other companies providing essential services to maintain the internet access situational awareness information from the CISCP?

3) Cyber Security Advisors (CSAs) connect critical infrastructure entities with the NCCIC information sharing programs. Additionally, CSAs help stakeholders learn about and join the CISCP, which provides a trusted forum where vetted partners share threat and incident information with the government and other private sector partners.
    a. Does the Department do targeted outreach based on its knowledge of interdependences and cascading impacts among critical systems that are the backbone of the internet?
    b. How many CSAs are dedicated to providing direct outreach to Managed DNS providers, cloud providers and other companies providing essential services to maintain the internet?

4) In the wake of the October 21st attacks, do you anticipate taking steps to enhance the reach of your Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division, which is supposed to be the primary point of engagement and coordination for national security communications and cybersecurity initiatives targeted at industry partners? If so, please elaborate.

---

[5] National Cybersecurity and Communications Integration Center, October 21, 2016.

5) The malware believed to be used in this attack, Mirai, exploits Internet of Things (IoT) devices, such as surveillance cameras and entertainment systems connected to the Internet, to carry out DDoS attacks. I am pleased that you announced that the Department is working to develop a set of principles for securing IoT in the wake of the Dyn attack.[6] Please provide the anticipated date of the release of the strategic principles for securing IoT.

Thank you for your attention to this matter. If you have any questions, please contact Hope Goins, Chief Counsel for Oversight at 202-226-2616.

Sincerely,

Bennie G. Thompson

BENNIE G. THOMPSON
Ranking Member

[6] "Statement by Secretary Johnson on Dyn Attack". October 24, 2016.