Testimony of Dale Drew
Chief Security Officer
Level 3 Communications

Before the

U.S. House of Representatives
Committee on Energy and Commerce
Subcommittee on Communications and Technology, and the
Subcommittee on Commerce, Manufacturing, and Trade

Joint Hearing Entitled
"Understanding the Role of Connected Devices in Recent Cyber Attacks"

November 16, 2016

Chairmen Walden and Burgess, and Ranking Members Eshoo and Schakowsky, thank you for the opportunity to testify on behalf of Level 3 Communications regarding the recent cyberattacks on our nation's communications landscape and the risks posed by vulnerabilities found in Internet of Things (IoT) devices.

Level 3 Communications is a Fortune 500 company that provides local, national and global communications services to enterprise, government and carrier customers. Level 3's comprehensive portfolio of secure, managed solutions includes fiber and infrastructure solutions; IP-based voice and data communications; wide-area Ethernet services; video and content distribution; data center and cloud-based solutions. Level 3 serves customers in more than 500 markets in over 60 countries across a global services platform anchored by owned fiber networks on three continents and connected by extensive undersea facilities.

Given our significant network footprint and the amount of traffic we handle on a daily basis, Level 3 has a unique perspective on the threats facing our communications landscape. To address the growing extent of cybersecurity risks, several years ago Level 3 established the Threat Research Labs to actively monitor communications for malicious activity, helping to detect and mitigate threats to our networks, our customers, and the broader internet. Every day, our security team monitors more than 48 billion security events, detecting more than 1 billion unusual or suspicious pieces of traffic.

The proliferation of IoT devices represents tremendous opportunities and benefits for consumers by connecting devices such as cameras, lightbulbs, appliances and other everyday items to the internet. Estimates suggest there are already billions of IoT devices in operation and their use is growing dramatically. However, the lack of adequate security measures in these devices also poses significant risks to users and the broader internet community.

Vulnerabilities in IoT devices stem from several sources. Some devices utilize default and easily-identifiable passwords that hackers can exploit. Others utilize hard-coded credentials that users are not able to change. Many devices also lack the capability of updating their firmware, forcing consumers to monitor for and install updates themselves. The global nature of the IoT device marketplace means many products are manufactured in and shipped to foreign countries that have yet to embrace sound cybersecurity practices. IoT devices also are particularly attractive targets because users often have little way to know when they have been compromised. Unlike a personal computer or phone, which has endpoint protection capabilities

and the user is more likely to notice when it performs improperly, compromised IoT devices may go unnoticed for longer periods of time.

In September 2016, Level 3's Threat Research Labs began tracking a family of malware targeting IoT devices. The bad actors were leveraging the infected devices to create Distributed Denial of Service (DDoS) botnets impacting not just those devices, but potentially anyone on the internet. The new malware known as Mirai and its predecessor BASHLITE has affected nearly 2 million devices on the internet. Mirai was used to attack the website KrebsOnSecurity.com as well as the Domain Naming System (DNS) company Dyn that compromised multiple major websites. These new attacks are alarming for their scope, impact, and the ease with which attackers employed them. Also worrisome is that these attackers relied on just a fraction of the total available compromised IoT nodes in order to attack their victims, demonstrating the potential for significantly greater havoc from these new threats. Level 3 detected approximately 150,000 IoT devices were used to generate more than 500 gigabits per second of traffic, a significant amount of bandwidth use that threatens the fabric of the global internet.

The primary motivation for these attacks appears to be financial. Hackers utilize DDoS to overwhelm a business, threatening to take their business offline unless they pay a ransom to the attacker. According to one estimate, the total costs of ransomware to U.S. businesses are expected to total $1 billion in 2016. In other cases, attackers are simply out to create mischief. We believe that in the case of Dyn, the relatively unsophisticated attacker sought to take offline a gaming site with which it had a personal grudge and rented time on the IoT botnet to accomplish this.

Level 3 is taking a number of steps to address these threats. In these recent IoT botnet attacks, Level 3 was not a direct victim of the attacks, but we see the devastating potential of what these unprotected IoT devices can bring, and we have decided to be proactive about protecting our backbone, our customers, and the global internet as a whole. We have contacted manufacturers of compromised devices to inform them of the problem and take appropriate action, such as firmware updates or recalls. We have engaged in a public awareness campaign to educate consumers and businesses about the risks of IoT botnets and steps they can take to protect themselves, such as updating the default passwords and downloading patches. We are working collaboratively with our industry partners to monitor this evolving threat and mitigation techniques. We also have actively been blocking critical elements of the IoT botnets in an effort to disrupt their communication.

With the exploding proliferation of IoT devices, so too will the threats they pose continue to expand and evolve. Bad actors are increasingly attracted to IoT devices since they can use those devices without being detected for long periods of time, they know most devices will not be monitored or updated, and they know there are no endpoint protection capabilities on IoT devices that can detect and remove the threats. Network operators, device manufacturers and users will need to remain vigilant to the security risks these devices present. The current lack of any security standards for IoT devices is certainly part of the problem that ought to be addressed. In particular, IoT manufacturers and vendors should embrace and abide by additional security practices to prevent harm to users and the internet. In this context, there may be a role for the government to provide appropriate guidance. It will be imperative for all relevant stakeholders

to continue to work collaboratively to address and mitigate IoT security risks so that we can reap the benefits of this exciting and transformative technology.

Thank you again for the opportunity to testify and I look forward to taking your questions.

###