Opening Statement of the Honorable Michael C. Burgess, M.D.
Subcommittee on Commerce, Manufacturing, and Trade & Subcommittee on Communications and Technology
Joint Subcommittee Hearing
"Understanding the Role of Connected Devices in Recent Cyber Attacks"
November 16, 2016

Good morning and welcome to our joint hearing examining recent cyber-attacks. Several popular websites were knocked offline for a couple of hours on October 21, 2016. Hackers used malware to create a botnet, or massive group of compromised connected devices, to flood a domain server system with terabytes of traffic, overwhelming the system and preventing the server from responding to legitimate traffic.

In this case, the result was brief outages on consumer facing websites. However, the incident is unique in that it utilized armies of compromised devices, rather than computers and laptops, to launch attacks without the knowledge of device owners. Many of these devices are everyday household items – such as baby monitors, DVRs, and webcams – that many consumers do not realize need strong cyber protections.

But that is exactly why this attack, and others like it, has been successful. The malware that created this botnet spread to vulnerable devices by continuously scanning the Internet for Internet of Things systems protected only by factory default or manually-generated usernames and passwords.

The balance between functionality and security is not going to be resolved in the near term. Consumers want the newest and fastest device as soon as possible, but they have not employed adequate security protections. In fact, the most common password is the word password. The culture surrounding personal cybersecurity must change to ensure the Internet of Things is not vulnerable to a single insecure device.

The Subcommittee on Commerce, Manufacturing, and Trade has explored cybersecurity throughout a number of hearings, including our Disrupter Series.

Cybersecurity has been raised and discussed at each of these hearings. Government is never going to have the man power or resources to address all of these challenges as they come up—which is why we need industry to take the lead.

Recent attacks present a unique opportunity to examine the scope of the threats and vulnerabilities presented by connected devices and learn how stakeholders are considering these risks throughout the supply chain, as well as how consumers are responding in the market.
We have learned about a number of best practices, and standards-setting projects are on-going with various groups.

We are facing exciting growth in the connected device industry, but we also need to see meaningful leadership from industry about how to address these challenges.

###