TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
http://oversight.house.gov

Opening Statement
Ranking Member Robin Kelly

Hearing on "Cybersecurity of the Internet of Things"
Subcommittee on Information Technology

October 3, 2017

Chairman Hurd, thank you for calling today's hearing and thank you to our witnesses for being here today.

We are here to talk about a critically important bill and the security of IoT devices that the federal government uses.

Senators Warner and Gardner recently introduced S. 1691, the Internet of Things Cybersecurity Act to help ensure that federal agencies procure secure IoT devices. I have been working on the discussion draft of the companion bill. I want to thank the Senators for their continued leadership on this important cybersecurity issue.

IoT devices are incredibly helpful for American citizens, businesses, and our federal government. From drones to smart lightbulbs to connected cars, hundreds of millions of Americans benefit from these devices every day. In fact, we expect to have more than 20 billion internet-connected devices online by 2020. Unfortunately, the high demand and lucrative market for IoT devices has also attracted bad actors who crank out cheap products that are insecure, unreliable, and vulnerable to malware.

We all know the dangers posed by unsecured devices. Even the least tech-savvy among us learned about the consequences last October when a Distributed Denial of Service Attack or DDoS attack on DNS service provider Dyn shut down Internet access for millions on the East Coast. We learned that the attack was carried out by a botnet composed of thousands of compromised IoT devices. It was a sobering reminder that everyday appliances like webcams, Smart TVs, and even thermostats can be turned into cyber-weapons.

There is no doubt that these attacks will grow in frequency and severity. The proliferation of IoT devices makes THESE attacks that much easier. It is estimated that October's Dyn attack only used a fraction of the botnet's capabilities. We can only imagine the disruption that a larger cyber-attack would cause – lives are at stake in this matter.

Given the gravity of this situation, Congress must be concerned about both disruptive cyberattacks and protecting sensitive data. Compromised devices can become access points for malicious actors to gain entry to the federal government's networks.

S. 1691 and my draft companion bill bake security into the procurement process. These bills ensure that procured devices meet minimum security requirements. We are talking about basic cyber-hygiene like ensuring that devices are patchable, that they do not contain known vulnerabilities or hard-coded passwords.

The legislation also provides agencies with flexibility to waive these requirements, if they employ similar requirements or use third-party device certification standards. These requirements make our agencies more secure while providing flexibility to vendors and agencies. We cannot predict the future of technology, which is why my discussion draft also includes the creation of an Emerging Technologies Advisory Board to review and provide recommendations to update guidelines in real time to address emerging threats.

Importantly, these bills are not meant to provide extensive, in-depth regulation. Sector-specific regulators will devise more precise rules to address the unique risks to each sector. Instead, they would establish minimal, flexible standards for government procurement of IoT devices.

I've long said that the federal government must be a leader in cybersecurity. This legislation takes us closer to that goal.

But my bill draft is not finished – we need the input of people like our witnesses, other stakeholders, and the public to make my bill as strong as possible so that our federal agencies can be safe and secure. It is a fine line to walk to secure our IT systems while encouraging innovation. I hope that at the end of this process we will have struck this perfect balance.

I look forward to hearing the witnesses' ideas and contributions to strengthen this bill.

Thank you, Mr. Chairman.

Contact: Jennifer Werner, Communications Director, (202) 226-5181.