NEAL R. GROSS & CO., INC.

RPTS SALANDRO

HIF164160

PROMOTING SECURITY IN WIRELESS TECHNOLOGY

TUESDAY, JUNE 13, 2017

House of Representatives

Subcommittee on Communications and

Technology

Committee on Energy and Commerce

Washington, D.C.

The subcommittee met, pursuant to call, at 10:00 a.m., in Room 2322 Rayburn House Office Building, Hon. Marsha Blackburn [chairman of the subcommittee] presiding.

Members present: Representatives Blackburn, Lance, Shimkus, Olson, Kinzinger, Bilirakis, Johnson, Flores, Brooks, Collins, Cramer, Walters, Costello, Doyle, Welch, Clarke, Loebsack, Ruiz, Dingell, Rush, Eshoo, Butterfield, Matsui, McNerney, and Pallone (ex officio).

Staff present: Kelly Collins, Staff Assistant; Blair Ellis,

Digital Coordinator/Press Secretary; Chuck Flint, Policy Coordinator, Communications and Technology; Gene Fullano, Detailee, Communications and Technology; Jay Gulshen, Legislative Clerk, Health; Kelsey Guyselman, Counsel, Communications and Technology; Lauren McCarty, Counsel, Communications and Technology; Paul Nagle, Chief Counsel, Digital Commerce and Consumer Protection; John Ohly, Professional Staff, Oversight and Investigations; Dan Schneider, Press Secretary; Jeff Carroll, Minority Staff Director; Alex Debianchi, Minority Telecom Fellow; David Goldman, Minority Chief Counsel, Communications and Technology; Jerry Leverich, Minority Counsel; Lori Maarbjerg, Minority FCC Detailee; Jessica Martinez, Minority Outreach and Member Services Coordinator; and Dan Miller, Minority Policy Analyst.

Mrs. Blackburn. --everyone, and go ahead and call our subcommittee to order. And I will begin by thanking Mr. Doyle's Penguins for a very fine hockey series against my Nashville Preds. I told him I thought about bringing him a little bit of catfish today, but we were sorry we didn't win but we think it was just a fantastic series and we congratulate.

Mr. Doyle. Well, thank you.

Mrs. Blackburn. Yeah. And now I recognize myself for 5 minutes for an opening statement. And I welcome each of you to the subcommittee's hearing titled, Promoting Security in Wireless Technology, and thank you to our witnesses for appearing and for offering your testimony on this important issue and thank you for submitting that testimony on time. We appreciate that.

Mobile connectivity has become essential to our daily lives as a result of technology and consumer demand. Unfortunately, increasing reliance on wireless devices and networks has provided more avenues for cybercriminals to compromise our security and harm consumers. According to the 2017 Hiscox Cyber Readiness Report, cybercrimes cost the global economy approximately 450 billion, and over 100 million Americans had their medical records stolen in 2016. I think that is such an important stat. 100 million Americans had their medical records stolen in 2016.

Threats to mobile devices and networks can run the gamut from the use of ransomware and phishing schemes to packet sniffing and

attacks on encryption protocols used to protect information sent over WiFi. These incidents have been occurring with alarming frequency on scales large and small. The Harvard Business Review wrote last September 22nd that--and I am quoting.

Mobile devices are one of the weakest links in corporate security and that if mobile security isn't a problem for your company yet, it will be.

Hackers are smart. They are adapting. McAfee's 2016 Mobile Threat Report notes mobile devices are quickly becoming the cybercriminal's target of choice because of the abundance of sensitive information individuals store on them. This is corroborated by a Newsweek report from March that stated mobile ransomware attacks had already grown over 250 percent in 2017. The sophistication and frequency of cyber attacks against mobile devices continues to escalate and we must meet this challenge head-on.

Our hearing will also examine threats to wireless networks. As the Majority Memorandum notes, mobile devices generate numerous air interfaces to transmit data, with each interface creating unique security vulnerabilities and attack methods. Threats include packet sniffing, rogue access points, jamming, and locating flawed encryption algorithms. These attacks can be initiated by hackers to obtain financial information, user passwords, and block legitimate network traffic. A recent

example of this was the DDOS attack against Dyn which disrupted websites such as Twitter, Netflix, and Etsy last November. We all remember that one.

I have often said that cyberspace is the battlefield of the 21st century. It is time to act. Hardworking taxpayers are demanding leadership from Washington in the cyber arena and it is our duty to provide it. Enhanced defensive capabilities should be developed by promoting greater collaboration between public and private entities.

CTIA has shown leadership through its Cybersecurity Working Group. Their efforts have brought federal agencies such as the FCC and DHS together with the private sector to develop solutions to the dilemma. Whether it is encryption, the use of authentication standards, updating operating systems, or rigorous implementation of anti-virus software, we must have an all-of-the-above approach when it comes to forging defensive strategies against cybercriminals.

I thank you all for being here and at this time I yield 5 minutes to the ranking member, Mr. Doyle.

[The prepared statement of Mrs. Blackburn follows:]

**********COMMITTEE INSERT 1**********

Mr. Doyle. I thank you, Madam Chair, for holding this hearing and for the witnesses for appearing today. Before I get started I just want to reiterate a momentous occasion in our city. The Pittsburgh Penguins have brought the Stanley Cup back to Pittsburgh for the second year in a row. We beat back broken bones and sideline starters and some ferocious play from the Nashville Predators. I know the Predators aren't squarely in the gentlelady from Tennessee's district, but I want to congratulate her and their team on a hard fought series.

Mr. McNerney. Will the gentleman yield to someone from the Golden State?

Mr. Doyle. No. No, I will not. But I have time at the end. You know, in Pittsburgh we could throw Primanti Bros. sandwiches on the ice but they taste so good we prefer to eat them. So anyways, go Pens and congratulations to the Predators.

I also want to mark another milestone. As of today, there are just under five million comments in the FCC's proceeding to repeal net neutrality rules. With still months to go, we have already far eclipsed the record-breaking 3.7 million comments that were filed in 2015. The vast majority of these comments are overwhelmingly in support of the current rules and opposed to the Trump administration's effort.

And I would once again urge the chairman to bring the Commission before this committee for oversight hearings so that

Congress can do its job and provide much needed oversight and public scrutiny. I think it would be a dereliction of duty not to provide oversight of an agency whose actions risk upending the internet ecosystem, one of the primary drivers of our economy.

Considering the number of oversight hearings held during the previous administration, I am sure my colleagues on the other side of the aisle appreciate this fact all too well and will see fit to schedule oversight hearings of the Commission as soon as possible.

Now, on to the topic before us today, promoting online security. Security is an absolutely critical issue. It enables an environment where commerce, communication, and innovation can flourish. However, increasingly, organizations are facing mounting threats and greater challenges particularly as more sectors of our economy come to depend on the digital infrastructure.

These challenges are being compounded by highly sophisticated online threats that are increasingly funded and supported by hostile nations. As the witnesses point out in their testimony, attacks we face today are highly sophisticated and increasingly destructive, from Crash Override to Mirai botnet, from the hacks of the DNC and the Russian meddling in the U.S. election to WannaCry ransomware, these issues are only escalating in their severity.

My colleagues, Representatives Clarke, Engel, and McNerney have all introduced legislation in this committee to address the threats we face. I would encourage the chairman to hold legislative hearings on these bills. I would also add that we need to use every tool in our toolbox to address cyber threats we are facing.

In repealing the FCC's privacy rules using the CRA, Congress also repealed data security protections contained in those rules. While these rules were not a panacea, they required reasonable steps to protect data and were a meaningful step towards addressing this issue.

With that I would yield the remaining minute and 35 seconds of my time to any one of my colleagues that desires to use it. Mr. McNerney?

[The prepared statement of Mr. Doyle follows:]

**********COMMITTEE INSERT 2**********

Mr. McNerney. Well, I thank the ranking member. And I don't want to say too much more about the Golden State Warriors so I will move on. But I want to thank the chair for today's hearing.

The security is important. Last October we witnessed a catastrophic attack that used the insecure Internet of Things devices to cripple the internet. A weak device security poses serious threats to our national security and to the economy. That is why I introduced the Securing IoT Act which would require that cybersecurity standards be established for IoT devices and that these devices be certified to meet those standards.

I am also disappointed that my Republican colleagues have not shown any interest in this bill especially since 20 to 50 billion connected devices are expected to be in use by the year 2020. Meanwhile, my Republican colleagues passed the privacy CRA, which leaves consumers more vulnerable to cybersecurity attacks, and that is why I introduced MY DATA Act so that consumers can have strong, data security protections.

I hope my colleagues can get behind these two important bills, and I yield back to the ranking member.

[The prepared statement of Mr. McNerney follows:]

**********COMMITTEE INSERT 3**********

Mr. Doyle. And Ms. Eshoo, would you like the remaining time?

Ms. Eshoo. Well, you are nice but there is 11 seconds left, so I will weave my comments in later on. Thank you very much. I appreciate it.

Mr. Doyle. Okay, thank you. I will yield back. Thank you.

Ms. Eshoo. Thank you.

Mrs. Blackburn. The gentleman yields back. Mr. Lance, you are recognized for 5 minutes.

Mr. Lance. Thank you, Chair Blackburn. And welcome to our distinguished panel, thank you for appearing before us today.

Since the advent of the smart phone and network innovations such as 4G LTE, consumers have become increasingly less constrained by location when using the internet. Mobile technology has changed the way consumers interact, freeing them to conduct business, to shop, to have access to health and financial records, to study and participate in countless other activities almost anywhere in the country.

As more and more technological innovations such as 5G and Internet of Things devices come to market, billions more devices will become connected and continue to revolutionize the way consumers and businesses behave. And we have just participated downstairs in a forum regarding the Internet of Things with many of the great companies in this country, including Qualcomm and Panasonic and Siemens and Honeywell and others.

However, with increased ease of access and reliance on connected devices comes increased security risks as the chair has already indicated. We have already seen bad actors take advantage of the flood of internet-connected devices in the DDOS botnet attacks last year, and an increase of phishing and malware attacks on mobile devices. Threats are constantly evolving and increasing in sophistication and scope.

Cybersecurity needs to be a priority as we become more dependent on connected devices. A large part of this is educating consumers and businesses on how best to protect themselves and their devices on the internet such as recognizing an attempt to invade the internet and regularly to change passwords.

There is also a responsibility for the government and industry to work together in making sure that networks and consumers are protected without mandating innovation-stifling technology or security standards that will become obsolete quickly. And we have seen this across the last 20 years that technology outstrips what we do here in Washington.

I thank our panel for your efforts in this important field and look forward to the testimony. And I apologize. I will be moving in and out. There are two subcommittees of importance today from the Energy and Commerce Committee. Certainly this is an incredibly important issue and I will certainly be here to the greatest extent possible.

Welcome again to our distinguished panel, and I would yield 2 minutes 20 seconds to any of our colleagues who wish to be recognized.

[The prepared statement of Mr. Lance follows:]

**********COMMITTEE INSERT 4**********

Mrs. Blackburn. Anyone seeking time for an opening statement? If not, the gentleman yields back.

Mr. Lance. I yield back, Madam Chair.

Mrs. Blackburn. Mr. Pallone, the ranking member of the full committee, you are recognized for 5 minutes.

Mr. Pallone. Thank you, Madam Chairman.

Cyber attacks are one of the most serious threats to our national security today. Every day, new information comes out about how the Russians and other foreign actors are hacking our institutions and our democracy. Just last week, former FBI Director Comey testified, and I am quoting.

The Russians interfered in our election during the 2016 cycle. They did it with purpose. They did it with sophistication. They did it with overwhelming technical efforts. It was an active measures campaign driven from the top of that government. There is no fuzz on that. Unquote.

This committee has primary jurisdiction over the communications networks that were used by the Russians to commit these attacks. We should be focused like a laser on how to stop them from happening again, but this committee has yet to hold a single hearing on these Russian hacks. Worse still, the only legislation House Republicans have pushed and supported within this subcommittee's jurisdiction actually makes us less safe, in my opinion.

With no hearings or advance notice, the leadership of this committee led the charge to strip away Americans' privacy rights and throw out some of the only protections on the books to secure our data. These safeguards simply said that broadband providers needed to take reasonable measures to secure Americans' data. But despite the Russian hacks, congressional Republicans eliminated those protections under the absurd pretext that asking companies to act reasonably was government overreach.

This hearing today is another example of committee Republicans simply not taking these issues seriously. Democrats tried to invite another cybersecurity expert to testify here today who could have helped us better understand the threats to our country like the Russian hacks, but the majority made up arbitrary and partisan reasons, in my opinion, to effectively block us. This decision shortchanges our members' ability to hear from the experts in this area. These games have to stop because these issues are just too serious to keep playing politics with our national security. Now Democrats are trying to address these issues head on in a nonpartisan way. We have put forward three bills--from Mr. Engel, Mr. McNerney, and Ms. Clarke--to help fix some of these problems.

These are good bills that were introduced more than 3 months ago and every day that goes by with no action is another day that the American people are at risk. Republicans, as I said before,

should stop playing political games with national security because the risks are too great. And with that I would like to yield the time that I have left to Ms. Clarke and Ms. Eshoo. I guess we will split it evenly. We will start, I yield to Ms. Clarke.

[The prepared statement of Mr. Pallone follows:]

**********COMMITTEE INSERT 5**********

Ms. Clarke. First, I would like to thank our ranking member, Mr. Pallone, for yielding his time to me and thank Ranking Member Doyle and Chairwoman Blackburn for holding this important hearing. And I welcome our witnesses today for their expert testimony, I look forward to hearing from today's panelists.

Many of my constituents in the 9th congressional district of New York have voiced their concerns on cybersecurity and have asked that I and my colleagues what we can do to lessen their vulnerability to cyber attacks which is why I introduced the Cybersecurity Responsibility Act of 2017.

The Cybersecurity Responsibility Act of 2017 calls on the Federal Communications Commission to take an active role in protecting communications networks by carefully arranging, organizing, and supervising cybersecurity risks to prevent cyber attacks. As technology continues to develop and grow, so must our rules and regulations on internet safety. It is our duty not only as Members of Congress but as members of the committee to protect Americans against cyber attacks by ensuring that there are sufficient rules in place. With that, Mr. Chairman, I yield back to you.

[The prepared statement of Ms. Clarke follows:]

**********COMMITTEE INSERT 6**********

Mr. Pallone. I yield the remaining of the time to Ms. Eshoo.

Ms. Eshoo. I thank the ranking member and I thank all the witnesses. Some of you have been here before, welcome back, and to those who haven't, welcome.

It has been said but it needs to be restated, cybersecurity, I think, is really one of the most pressing national security issues, challenges for our country. Almost everything that we do here in Congress relative to cybersecurity is after there has been a breach, and I think that we need to really drill down on prevention.

I have spoken to countless people in my Silicon Valley district. Almost to a person they tell me that we need to concentrate on prevention. Up to 90 percent of the breaches, both government and private sector--and 95 percent of this is private sector, 5 percent is the Federal Government as important as it is--say that there are two pillars to this. One is cyber hygiene and the other is consistent security management, so I am shortly going to be introducing legislation that reflects that.

I think that NIST can set the standards and I think that companies should have a set of good housekeeping seal of approval and that as important as it is to take steps after something has happened, I think that we need to start focusing on prevention.

So we will talk more about it with our distinguished panel, but I want to thank the ranking member for allowing me to, giving

me some time to make this brief statement. Thank you.

[The prepared statement of Ms. Eshoo follows:]

**********COMMITTEE INSERT 7**********

Mrs. Blackburn. The gentlelady yields back. The gentleman yields back and this concludes our opening statements. I will remind all members that their opening statements will be made a part of the record.

And we do thank our witnesses for being here with us today. We are going to give each of you the opportunity to make a 5-minute opening statement.

And our witnesses, Mr. Bill Wright who is the director of Government Affairs & Senior Policy Counsel, and we welcome you; Mr. Amit Yoran who is the chairman and CEO of Tenable; Ms. Kiersten Todt who is the managing partner at Liberty Group Ventures and a resident scholar at the University of Pittsburgh--I guess you are celebrating too--Institute for Cyber Law, Policy, and Security; and Mr. Charles Clancy who is the director and professor at Hume Center for National Security and Technology at Virginia Tech.

So we appreciate that you are each here. We will begin, Mr. Wright, with you. You are recognized for 5 minutes for your opening statement.

STATEMENTS OF BILL WRIGHT, DIRECTOR, GOVERNMENT AFFAIRS & SENIOR POLICY COUNSEL, SYMANTEC; AMIT YORAN, CHAIRMAN AND CEO, TENABLE NETWORK SECURITY; CHARLES CLANCY, DIRECTOR AND PROFESSOR, HUME CENTER FOR NATIONAL SECURITY AND TECHNOLOGY, VIRGINIA TECH; AND, KIERSTEN TODT, MANAGING PARTNER, LIBERTY GROUP VENTURES

STATEMENT OF BILL WRIGHT

Mr. Wright. Chairman Blackburn, Ranking Member Doyle, members of the subcommittee thank you for the opportunity to testify today. The cyber threats that we face today and every day are growing both in numbers and in sophistication. As the chairman pointed out in her opening statement, cyberspace truly is the battlefield of the 21st century.

And while global ransomware attacks and destructive malware attacks tend to steal the headlines, it is other threats--threats to mobile, threats to wireless, threats to IoT--that are quickly gaining prominence. And no wonder, today more than half of the world's web traffic originates from mobile phones and nearly half of the people on the planet own a smart phone today.

But I think calling it a phone doesn't quite do this justice. This isn't a phone. It is a powerful, connected, handheld computer and from time to time you can use it to call your wife. We need to start viewing these as computers and we need to protect

them as computers. Our web searches, our banking, our personal health information is all being transmitted and stored on mobile devices. Our smart phones are becoming an extension of ourselves and our identity.

We are also seeing a blurring of the lines between work-issued devices and personal devices. Employees can and often expect to be able to work from anywhere. Workers can unwittingly introduce virus into an entire network system from a single download of a malicious app. IT security is no longer about just protecting the perimeter from attack because that perimeter now covers the entire planet.

As we all rush and rush to connect more and more devices to the internet we will undoubtedly improve our lives in many, many ways, but we will also be greatly increasing the attack surface. Last year's Mirai botnet DDOS attack was a sobering wake-up call for how powerful IoT-based botnet could be. And it was also a chilling reminder for what could happen if those bot masters had trained their sights elsewhere, say on an industrial control system.

Attackers are continuing to evolve their criminal tools and getting better at avoiding detection and obfuscating their actions. The incentives for criminals is very strong. Cybercrime is more lucrative than ever. There is very little risk in getting caught and the underground cybercrime marketplace is

booming, allowing even an art history major to conduct highly sophisticated cyber attacks by renting crime as a service by the hour or buying ransomware tool kits or mobile banking trojans.

Mobile device manufacturers, particularly Apple, have done a pretty good job at putting security into their products and keeping malicious apps out of their stores. Android also has made some great strides over the last year. However, the very attributes that make mobile phones so attractive to consumers also make them a very tempting target for cybercriminals because unlike your desktop computer, your mobile device is always active, always receiving and used for every aspect of your life.

Increasingly, smart phones are used for authentication purposes in various online accounts. A hacker only needs to steal or access your mobile device to get past all the other defenses that have been set up on the network side. Unfortunately, the public's attitude towards securing their devices has not kept pace with the potential threat. More than a quarter of smart phone users do not even use the most basic security feature, the screen lock, let alone applying timely software updates.

And the criminals are following their victims onto these new platforms. Over the last few years we have seen a dramatic rise in malicious activity related to mobile devices driven by cybercriminals using tried and true methods to monetize attacks such as premium text messages, click fraud, and ransomware. Last

year, Symantec detected more than 18 million mobile threats, an increase in 105 percent from the prior year. This trend will only be exacerbated over the next few years when tens of billions of connected devices are added to the internet. Cybercriminals are only bound by their own imagination and if there is a way to steal valuable data and monetize it, they will find it.

As this subcommittee knows, we face significant challenges in our efforts to secure wireless networks and mobile devices and while there remains much work to be done we have made some progress in some areas, for instance, how we share threat information and when we share threat information with our government partners.

At Symantec we are committed to improving online security across the globe, including wireless and mobile security, and will continue to work collaboratively with our customers, industry, and governments to do so. Thank you again for the opportunity to testify and happy to answer any questions.

[The prepared statement of Mr. Wright follows:]

**********INSERT 1**********

Mrs. Blackburn. I thank you for the testimony.

Mr. Yoran, you are recognized for 5 minutes.

STATEMENT OF AMIT YORAN

Mr. Yoran. Chairman Blackburn, Ranking Member Doyle, and members of the subcommittee thank you for the opportunity to testify today in what promises to be the most exciting hearing of the day. I am chairman and CEO of Tenable, the world's most widely deployed vulnerability management solution including in the Federal Government where the majority of government agencies use our technology to assess and manage their cyber risk.

It is important to put mobility and wireless in the context of modern computing enterprise environments which are dynamic and borderless and virtually unlimited in connectivity. Mobile devices, wireless networks, transient user populations, cloud-based infrastructure, web applications, and the shift to DevOps go hand in glove with the Internet of Things in invading our computing environments.

Today's complex mix of computer platforms and applications combine to represent the modern attack surface where the assets themselves and their associated vulnerabilities are constantly expanding, contracting, and evolving, almost like a living organism, creating gaps in overall system understanding, security coverage, and resulting in underestimated exposure. Therefore, it is important that any approach to cybersecurity for mobile devices or wireless networks not be done in isolation but, rather,

viewed as part of a holistic ecosystem.

In over 20 years practicing information security, the following axiom proves true time and again. You cannot secure what you don't know about. If there are elements of your computing environment that are invisible or unknown to you, chances are that they represent unaccounted-for risk.

Both the NIST Cybersecurity Framework and DHS's Continuous Diagnostics and Mitigation program call for identifying assets and vulnerabilities as the first step in cybersecurity. Identifying assets not just once but continually is foundation to assessing risk and developing effective security programs. My written testimony includes policy recommendations, a few of which I will highlight. First, we need a bold, new cyber workforce strategy that develops and advances the ranks of all people from different walks of life. Only through increased inclusion and diversity in perspective and thought can our industry achieve the greater creativity, innovation, and develop new solutions to our most vexing challenges.

At Tenable we have implemented a Rooney Rule to set an example of greater diversity in our leadership ranks. I do want to state however that our efforts to expand the workforce will inevitably fall short of the insatiable demand for cyber talent and we have to prepare for that with a complementary focus on technology and automation.

Second, the government should encourage the private sector companies to continually and fully assess their cybersecurity risk just as the federal agencies will be doing and many regulatory requirements and best practices already mandate. Today, all organizations are part of a global ecosystem with a cyber hygiene responsibility to one another. Simple malware like WannaCry demonstrated what a very crippling cyber attack might do. The infection was spread company to company, many of which simply failed to adequately assess their cyber risk and act accordingly. Third, the Federal Government should continue to promote the NIST Cybersecurity Framework which, according to Gartner, will be adopted by 50 percent of organizations by 2020.

In closing, I want to emphasize the importance of taking an agile, continuous, and holistic approach to cybersecurity and technology policy. As we all know, IT is changing quickly across so many different dimensions. Prudence would have us look at mobile devices, wireless networks, and other technologies gaining great adoption in the broader context of our IT environments rather than in isolation.

I would like to thank Chairman Blackburn, Ranking Member Doyle, and all the members of the subcommittee for their attention to this important issue and I will be happy to respond to your questions.

[The prepared statement of Mr. Yoran follows:]

543

544 **********INSERT 2**********

Mrs. Blackburn. I thank the gentleman and he yields back and, Dr. Clancy, you are recognized for 5 minutes.

STATEMENT OF CHARLES CLANCY

Mr. Clancy. Thank you, Chairman Blackburn, Ranking Member Doyle, and members of the subcommittee. I think that you have a heard a lot about the threats that we face in the wireless security space.

Mrs. Blackburn. Your microphone.

Mr. Clancy. Oh, sorry. Thank you, Chairman Blackburn, Ranking Member Doyle, and subcommittee members. I think we can all agree that there are major vulnerabilities in the larger ecosystem of wireless security that we have reason to be concerned about. I would like to focus my opening remarks a bit on the wireless infrastructure that underpins those networks.

Over the last decade we have seen a fundamental shift of the DNA of the internet from the internet that connected stationary computers to fixed server infrastructure to one that is the social mobile internet. It is ubiquitous mobile broadband that connects smart phones and users to social media and the internet as a whole.

This has again fundamentally changed the makeup of the traffic on the internet and the nature of the cybersecurity threat to the internet. Over the next decade we will see another titanic shift of the internet with the so-called Internet of Things which has been referred by several others so far, but the idea here is that we could see an increase of 20 billion devices connected to

the internet; again another fundamental titanic shift of the DNA of the internet.

The wireless industry is working aggressively to address the needs of IoT with 5G wireless technology and is seeking to make sure that there are security components that are built into the infrastructure to address those needs. If you look at our cellular infrastructure today, the majority of us have 4G LTE coverage.

And 4G LTE learned from the mistakes of 3G, which learned from the mistakes of 2G, which learned from the mistakes of 1G, and for the most part has the needed building blocks to develop and manage a secure, wireless, mobile broadband infrastructure. The key challenge we have though is that while 4G LTE is ubiquitously deployed, we still have 2G and 3G infrastructure that is operating, and much of the rest of the world has 2G and 3G infrastructure operating that remains vulnerable to a wide range of different attacks.

And in particular, in the last 12 months we have seen press around IMSI catchers or so-called StingRays that are able to compromise user privacy and the SS7 attacks that were able to impact user privacy as well. And the big challenge is not that 4G LTE is insecure, it is just that we still have this legacy 2G infrastructure deployed that remains insecure.

Additionally, we have unlicensed bands, unlicensed

technology, wireless technology-fueled innovation over the last decade or two, right. WiFi fundamentally transformed many aspects of how we connect to the internet and how internet is available to us. However, in the early days of WiFi there were rampant security vulnerabilities. My Ph.D. dissertation was studying those vulnerabilities and looking to address them in the standards that ultimately became WPA and WPA2, which ultimately shored up many of those vulnerabilities.

And while home users and residential WiFi networks are for the most part secure through deployment of these new technologies, hotspots at everywhere from your coffee shop to airplanes remain insecure and are vulnerable to attacks that we have known about for 2 decades. So that remains, I think, a challenge as we look at the wireless ecosystem as a whole. Third, I would look at the services that operate over these networks, right. We have a very complex tapestry of members of this ecosystem. We have the device manufacturers, we have the operating system vendors, we have the people who write and develop apps that run on these systems. We have the cellular operators. We have the OEMs who build equipment for the cellular operators. We have the cloud providers and we have the median service entities that sit over top of all of it. And each of one of these different groups has a different regulatory focal point within the U.S. Government, whether it be the Federal Communications Commission or the Federal

Trade Commission or DHS, and this creates a very complex ecosystem when seeking to achieve cybersecurity because no one entity across that entire continuum has enough control of the ecosystem to achieve unilateral security.

So as a result, I think it is imperative that we look at cybersecurity as a partnership where we need stakeholders across all the, both government and industry to be working together on developing solutions and deploying those solutions.

And lastly, as a member of the academic community, I will reinforce the points that have been made earlier around workforce. There are over a million cybersecurity jobs here in the United States of which 31 percent are vacant. The number of new jobs in cybersecurity each year that become open exceeds the total volume of computer scientists graduating across the entire United States.

So we need to think more broadly about how we fill these cybersecurity gaps, and we need to think of cybersecurity not just as a subdiscipline of computer science, but something that is fundamentally intrinsic to technology overall. And with that I will thank the chairman and conclude my remarks.

[The prepared statement of Mr. Clancy follows:]

**********INSERT 3**********

Mrs. Blackburn. The gentleman yields back and we thank you.

Ms. Todt, you are recognized for 5 minutes.

STATEMENT OF KIERSTEN TODT

Ms. Todt. Good morning, Chairman Blackburn and Ranking Member Doyle and members of the subcommittee. Thank you for the opportunity to present my testimony on the promotion of security in wireless technology. I am currently the managing partner of Liberty Group Ventures and a resident scholar in Washington, D.C. at the University of Pittsburgh Institute for Cyber Law Policy and Security.

I also serve on the Federal Advisory Board of Lookout, Incorporated, and most recently served from March 2016 to March 2017 as the executive director of the presidential Commission on Enhancing National Cybersecurity. This Commission was bipartisan independent and was charged with developing actionable recommendations for growing and securing the digital economy as well as for creating a road map for the incoming administration.

I appreciate this subcommittee's awareness of the need to focus on the security of wireless and mobile technology. In a world where first-to-market overrides secure-to-market and every enterprise is seeking to make operations move more quickly and be more convenient, addressing the security of these innovations is critical and absolutely necessary. In response to the questions posed by this hearing, my testimony will primarily focus on mobile security and addressing the growing threat around

interdependencies in IoT.

Mobile devices are an attack vector that cannot be ignored and they are increasingly targeted for access to sensitive information or financial gain, as we have heard thoughtfully from our other panelists. But mobility should not be at odds with security and the reality is that cloud and mobile adoption in the enterprise is just beginning. Mobile devices are a part of every supply chain in your home and in your office, and mobile devices have become much more than communications devices. They are the access point to our work and our personal lives. Additionally, with the rise of two-factor authentication -- an important step in ensuring security but not the ultimate solution -- the smart phone has become even more important than the password.

A compromised device could hand over to an attacker an authentication code and thus access to an individual's most personal information as well as any work related sensitive information. All mobile products have latent security vulnerabilities that could be exploited by bad actors and many users ignore security policies and download apps from unofficial sources.

According to a recent Ponemon study, 67 percent of the Global 2000 reported that a data breach occurred as a result of employees using mobile devices to access the company's sensitive and

confidential information. Last summer, Lookout and Citizen Lab detected the Pegasus spyware. Pegasus took advantage of three zero-day vulnerabilities in the iOS devices to take complete control of a device.

The attack was capable of getting messages, calls, emails, logs, et cetera from apps including Facetime, Facebook, WhatsApp, Viber, Skype, Gmail and others. This threat represents the first time anyone has seen a remote jailbreak of an Apple device in the wild and shows us that highly resourced actors see the mobile platform as a fertile platform for gathering information.

Historically, government agencies have been restrictive about the use of mobile devices in the workplace. Perhaps because agencies now recognize that mobility is happening with or without their permission, we are beginning to see a shift towards prioritizing mobility initiatives in the Federal Government. The bottom line is that smart phones are essentially a super computer, as my colleague Mr. Wright noted, and today most have absolutely no security software on them. Mandates or policies stipulating that mobile devices must have an agent on the device that does predictive analytics should be considered.

I would like to take this opportunity to commend John Ramsey the CISO of the U.S. House of Representatives for his focus and recent action on mobile security. This example is one where Congress is ahead of the executive branch in implementing a

cybersecurity best practice, and I encourage this committee, perhaps in collaboration with the House Homeland Security Committee, to hold a hearing on and to examine how federal agencies can do a better job to defend against mobile security risks and to take a page from the U.S. House of Representatives.

Our interconnections and interdependencies are becoming more complex and now extend well beyond critical infrastructure. These interconnections reduce the importance of the critical infrastructure label because by association all dependencies may be critical as we saw with the Dyn/Mirai attack last fall. The proliferation of IoT devices is a growing challenge, and for the purpose of this hearing I offer the automobile as an example of interconnected devices. A Tesla is really a giant phone and battery on wheels. The base technology for connected cars originates from the smart phone revolution. And IoT and all of the technology that goes into connected cars, for example, is based on open source code that is genetically related to smart phones.

We need to recognize that neither the government nor the private sector can capably protect systems and networks without close and extensive cooperation. The mobile environment only adds to the challenge and urgency to develop an approach that emphasizes pre-event collaboration, which I describe in my written testimony, to more effectively manage our collective

cybersecurity risk.

As Representative Eshoo noted, government does instant response well, but we need to be doing more to focus on prevention and collaboration before an event actually occurs. Information sharing is a byproduct of trust that develops through that type of collaboration. We now recognize mobile security as one of the greatest risks affecting all enterprises and we therefore need to treat mobile devices as an endpoint priority equal to, if not more important than, traditional endpoints such as desktops and laptops.

Thank you for the opportunity to testify in front of you today. I look forward to answering your questions.

[The prepared statement of Ms. Todt follows:]

**********INSERT 4**********

Mrs. Blackburn. Thank you so much. That was wonderful testimony, zipping right through it. And so we will begin with questions and I will yield myself 5 minutes and begin the questions.

Mr. Wright, I am going to start right there with you. We know and you all have referenced some of the public-private partnership, the government-industry partnerships that have moved forward and attempted to look at best practices in the mobile cyberspace. NIST, we have mentioned that a couple of times their framework and CTIA Cyber Working Group.

So is standard setting enough, is best practices enough, or do we still need to have a statutorial legislative solution?

Mr. Wright. Well, I think it might be a little early to tell.

Mrs. Blackburn. Microphone.

Mr. Wright. Oh, apologies.

Mrs. Blackburn. No problem.

Mr. Wright. I think it might be a little early to tell right now following some of the NIST and cybersecurity framework guidelines I think is working. I think there are a lot of private sector that are currently adopting part of the executive order. It is going to get more of the government using the NIST Cybersecurity Framework, but there is a lot of other cooperation going on between public and private sector as well.

I think if WannaCry had happened 2 years ago it would have

been a much different story. Today, this time you had government and the private sector coming together immediately within hours of the outbreak starting, sharing information, sharing indicators of compromise, and you ended up getting sort of a much, much better result.

At Symantec, I know we take our government and our private sector relationships very seriously, most oftentimes focused on law enforcement. But that sort of private sector industry and government partnering, I think, really is the key to this. There is no government around that is going to be able to fight this problem alone and there certainly is no private company that is going to be able to fight this alone.

Mrs. Blackburn. Okay. Anyone else want to add something? Ms. Todt?

Ms. Todt. If I may. So I had the privilege of working with NIST on the development of the Cybersecurity Framework, and one of the reasons why it continues to be so successful is it was developed by industry for industry, so then there is an approach that industry is then allowed to take to understand how to manage its risks.

And I think one of the strong points to the executive order that President Trump released was the focus on risk management, and I think when you are looking for industry and government to come together having that focus on risk management from a

collaboration perspective helps to develop those standards.

What we concluded in the Commission report was that private and public sector they should work together. When they don't work together we should create incentives and when those incentives don't work then we should interfere with regulation and other types of official standards.

Mrs. Blackburn. Okay, anyone else?

Dr. Clancy, let me ask you. You talked a little bit about the Internet of Things and the connected devices. And of course we have a forum going on today, a showcase dealing with some of that. I want you to expand a little bit on the challenges of securing the IoT devices, especially the wearable technologies, and what would be some of the consequences of our failing to adequately secure IoT devices if you have 20 billion such devices connected to the internet in a few years, and what do you see that framework, those challenges?

Mr. Clancy. Well, I think that IoT represents a breadth of different products and technologies. You have your internet-connected --

Mrs. Blackburn. Right, let's focus on the wearable technologies.

Mr. Clancy. Okay. So with respect to wearable, I think some of the chief concerns are privacy of individual users. And we want to make sure that data that is collected from those devices

and ingested into the cloud and used as part of whether it is some health app or some other service to consumers that that data remains private and isn't used to compromise the privacy that use that information.

I think some of the challenges we have are that much of the devices are manufactured overseas. We have supply chain challenges and code quality challenges with the software that is in those devices and that results in devices that we don't know if are robust or not. Many times they connect through unlicensed WiFi devices and there is no strong credentials or authentication that can be used to provide real governance over those devices. There is no way to push out software updates, for example, in a deterministic way if there are vulnerabilities that are discovered.

So I think those are some of the challenges that we face and particularly in the wearable space of IoT.

Mrs. Blackburn. Thank you. Before I yield back my time I will, my colleagues across the aisle have mentioned Russia a couple of times. And I would just like to highlight that we have in times past tried to raise Russia and our concerns there is an issue and indeed with items manufactured offshore, I think Huawei. We did a hearing on cyber and Huawei and concerns with Russia and then even in the 2012 Presidential Mr. Romney raised Russia as a concern.

I would also highlight with my colleagues we have privacy and data security legislation we would love to move forward on. We look forward to having them join us in working on these issues. And with that I yield back my time and recognize the gentleman from Pennsylvania for 5 minutes for questions.

Mr. Doyle. Thank you, Madam Chair. So as the threats we face continue to evolve and grow it seems that we not only need to step up our basic practices of cyber hygiene and best practices, but we need to look to the future. And the witnesses, all of you in your testimony, refer to the shortfall in the workforce for cybersecurity positions.

I know that DARPA in 2016 had the Cyber Grand Challenge and they challenged researchers to create autonomous systems that could defend against cyber attacks. Actually, a team from Carnegie Mellon won that challenge, a victory that we are proud of in Pittsburgh.

But I am curious. How does the panel see autonomous defensive systems addressing this escalation in threats in our workforce shortfalls? And we can just start at Mr. Wright and go down. Please.

Mr. Wright. Certainly the shortage in qualified cyber personnel is a problem today. It is going to be a problem in the future. I think the more that we can move toward autonomous defenses the better off we are going to be. I don't think the

technology is there today, but it is getting better every day. That type of innovation I know is a huge focus for not just for Symantec but for other vendors as well.

Mr. Doyle. Thank you. Mr. Yoran?

Mr. Yoran. I think that there is great promise and certainly progress being made in autonomous defenses, a lot of work going on in the cyber domain around artificial intelligence. From my perspective, the key to success is to scale the talent that we have asymmetrically. Part of that would be through autonomous defense, part of it would be through other technologies which provide the limited number of network defenders to cover more ground.

Mr. Clancy. I would agree with that. I think the major opportunity with autonomous defense is to act as a force multiplier for those human analysts who ultimately are making decisions about what defenses to deploy and how to manage them. We are seeing a renaissance of artificial intelligence right now with deep learning and early research. Applying that to cybersecurity looks very, very promising. But that will help make existing analysts and cyber defenders more efficient, but they will always still need to be part of the equation.

Mr. Doyle. Sure.

Ms. Todt. I would like to just approach it from a little bit of a different perspective in the sense that from the workforce

we look at the fact -- what we heard on the Commission particularly is that there are two issues. The current workforce that we have isn't trained effectively for the skill sets that are needed and we also need to be bringing in additional individuals into the workforce.

But this needs to happen while automation, AI, big data machine learning, are all being developed and so what we have to understand is that the culture of cybersecurity that is being created covers everything. And arguably, everybody is a part of the cyber workforce, so while developing that workforce we are also being able to invest in the innovation that can contribute to the autonomous defense that you mentioned.

Mr. Doyle. Thank you. Let me ask the panel this also. You know, as we look to the range of threats by government, industry, institution to individuals, we acknowledge we all have a shared responsibility to defend and protect this infrastructure. So what role do you think ISPs can play in mitigating cyber threats whether it be a botnet, malware, or some other threat, do you think federal agencies should have more authority to mandate either concrete steps or risk mitigation frameworks to ensure that these companies take sufficient steps to protect these networks if they are not doing it on their own? And for anyone on the panel.

Mr. Yoran. Sounds like a dangerous question. I will take a stab at it. I think that there is an opportunity for service

providers to differentiate themselves based on security service levels and we have seen a number of service providers take a very proactive approach to their security programs and offer security services and protective services as part of these packages and using it as a differentiation.

When you get to a point of mandating security, I think you are on a very slippery slope and potentially dangerous scenario where the service providers don't necessarily own the applications. They don't understand the ways the systems are being used and what impact might occur if they choose to block certain types of traffic or not.

So there is merit in further investigating the concept, I just think it should be done very cautiously.

Ms. Todt. And I just would like to add, from the executive order this was one of the key issues that was raised and it was also something that created a lot of initial tension with the Commission to understand whose role, who is responsible for what. As Amit said, I mean this is dangerous territory and there was a lot of discussion and debate.

But what the executive order lays out and I think what industry has said is essentially we need to come together to understand where the responsibilities lie and how to create a road map for moving forward. This is clearly an issue for collaboration between industry and government.

Mr. Doyle. Thank you. Thank you, Madam Chair. I yield back.

Mrs. Blackburn. The gentleman yields back. Mr. Lance, for 5 minutes.

Mr. Lance. Thank you. I promise no dangerous questions and you have all answered them very beautifully and very adeptly in my judgment.

Dr. Clancy, you mentioned in your testimony that 5G technologies have the opportunity to close current cybersecurity gaps. Can you please expand on what these cybersecurity gaps are and how the industry 5G innovations can help close the gaps?

Mr. Clancy. I think that as you look at the shift, the technology shift that has happened as we move from the 3G and 2G core network infrastructure to the 4G core network infrastructure, we have moved away from the old circuit switch technology and into all IP-based cell phone backhaul and backbone.

This is creating a range of new opportunities for new technologies and new services that can be provided through this infrastructure and it also exposes much of the cellular infrastructure to the same sorts of risks that you face on the internet. Before, we had a closed circuit switch network that was isolated from the internet; now the barrier between the internet and the cell phone core infrastructure begins to get blurry because of the structure of the 4G infrastructure.

5G actually blurs the line even further with technologies like edge computing, a cloud-based Radio Access Network technology. However, these are new tools in the toolbox that could be used to construct a better set of layered cyber defenses on behalf of subscribers, but we still haven't yet from a research and standards perspective really figured out how all of that will fit together.

Mr. Lance. Thank you. Mr. Yoran, as we saw with the attack last year, unsecured Internet of Things devices, can pose a threat to the other areas of the internet ecosystem. With billions of IoT devices expected to come to market in the coming years, it is essential that this vulnerability be addressed. Do you see the NIST Cybersecurity Framework as the best approach to address Internet of Things security?

Mr. Yoran. I think the NIST Cybersecurity Framework is probably the best place to begin the dialogue around Internet of Things security. At the end of the day, we have to take a holistic approach to cybersecurity. We can't look at multiple devices independently, we can't look at wireless networks independently or Internet of Things independently. These things are completely intertwined. Internet of Things most frequently rely on wireless networks for their communications so they have to be looked at.

And I think the most important thing from my perspective that the Cybersecurity Framework pushed toward was taking a risk-based

approach, because no use of technology is risk-free so understanding it from a risk perspective is really helpful.

Mr. Lance. Would anyone else on the panel like to comment?

Ms. Todt. Just a quick comment. That is one of the issues that was brought up also in the executive order and from the Commission which is to bring together, as Amit said, bringing together industry and government based off of the platform. So I think there is motion already in place at NIST to move forward with this to be able to create a set of standards that industry creates for itself.

Mr. Lance. I couldn't agree with that more in that industry is often ahead of us in government and we want to work in a cooperative way. But my belief, based upon the last 20 years, is that we are innovative because of the way we have approached this and certainly we want the United States to continue to be the innovative center of the world regarding these matters.

I represent a district that is very heavily involved in technology and in the internet and we want that to continue. We don't want to lose leadership to some other place around the globe. Thank you, Chair, and I yield back a minute.

Mrs. Blackburn. And we will take it. And Mr. McNerney, 5 minutes.

Mr. McNerney. I thank the chairwoman. Ms. Todt, in your written testimony you talked about the world where first to market

overrides secure to market. Would you agree that we are currently faced with a market failure since those who buy and sell insecure devices now have to bear the full cost of those devices?

Ms. Todt. So I think you have asked a question that is really at the crux of the IoT debate, because as long as we are pushing out innovation without any security guidelines or boundaries we are in this second phase.

A colleague of Mr. Wright's at Symantec was part of the NSTAC report who talked about this first 18-month window that we have passed on the proliferation of IoT devices. And where we are now is that we heard from, in one of our Commission hearings, the CIO of Intel who said we want regulations and standards around IoT devices because we can't possibly compete in this realm where you have small businesses pushing out the innovation.

So we have to think thoughtfully about incentives, penalties, and being able to truly develop secure by design, which is unfortunately becoming one of those terms that is losing its meaning because it is such a common term. But the idea of building security in and having to build software and hardware to certain standards around security has to be a priority right now with, as we have heard, all of the statistics the proliferation of IoT devices that is only going to increase.

Mr. McNerney. Well, you sort of answered my follow-up question already which was I proposed legislation that would

require cybersecurity standards to be developed for the devices and for the devices to be certified to meet those standards. Would that help decrease the threat?

Ms. Todt. So I think it actually connects back to an earlier question which is how do we build out the IoT standards? And I would offer that where we have seen such success with the NIST Framework is the fact that industry and government have worked together and so really looking at that collaboration first and foremost and then being able to inform any legislation.

I think the sequence of that is important because we learn from what industry has done and we have to come together to then develop the standards that you reference.

Mr. McNerney. Okay, thank you. Mr. Wright, Symantec's Internet Security Threat Report points to a growing number of attacks on IoT devices. Would requiring the IoT devices to meet baseline cybersecurity standards help decrease that threat? Is your microphone on?

Mr. Wright. It certainly would be something to look into. I also agree that the NIST Cybersecurity Framework is a good place to begin a lot of those discussions. IoT is a little bit strange. The consumer isn't really playing the role of demanding secure products at this point. Some of that could be around awareness. Thirty six percent of the devices that are being manufactured and pushed out there right now have a default password of ADMIN. Some

of these are very simple fixes. I think when the consumers are armed and aware of the dangers they have a better chance of driving some of those markets.

Mr. McNerney. Well, although the WannaCry ransomware attack was not the result of insecure IoT devices, I am curious about what lessons we can apply from the attack to IoT device security. How susceptible are IoT devices to ransomware attacks?

Mr. Wright. So we have seen some preliminary more like research around IoT. I know that smart -- we did a research project where a smart TV was hacked in ransomware. Like I said earlier in my testimony, criminals are looking for ways to monetize these attacks. They are only bound by their imagination and it is a matter of time before they are able to figure out how to monetize ransomware attacks on devices, on IoT devices.

Mr. McNerney. Well, are there a way that an IoT security or insecurity could result in physical harm?

Mr. Wright. Certainly. IoT devices that are infected can have real-world consequences, absolutely.

Mr. McNerney. And just to explain, how come it is difficult to patch IoT devices?

Mr. Wright. Well, a lot of times these are being shipped out without any possibility of sending out firmware changes. In fact, most of them cannot receive patches or updates.

Mr. McNerney. So could we, in your opinion, rely on

voluntary IoT device security from the manufacturers?

Mr. Wright. Well, I think that is -- I do think this needs to be sort of a consensus-driven standard. We need to have private sector involved. We need to have government involved and sort of find that middle ground, otherwise it is not going to work.

I will point out one thing. The Mirai botnet that we were discussing today, those devices were not manufactured in the U.S. but rather the vast majority of them were manufactured overseas, specifically in China.

Mr. McNerney. Okay. Before I yield I just want to say I appreciate Ms. Todt's remark that government does respond well but needs to do prevention better. Thank you. I yield back.

Mrs. Blackburn. Mr. Shimkus, you are recognized for 5 minutes.

Mr. Shimkus. Thank you, Madam Chair. And this is an excellent hearing. I do want to thank you all for coming. This is like an arms race. And the reason why I have always enjoyed this committee is that, you know, technology moves faster than we can regulate, hence it is very successful. Well, and that is part of this debate.

I mean, do we do federal standards and really almost slow up the ability for expansion and new applications or, and so that is why I like -- I think most people are talking about consensus base working with the sector, because if we don't we will trip

over ourselves and we will slow applications, we will slow development. And that is why I think you see us kind of doing this little kabuki dance between the sides because it is just a very exciting, but there is a lot of dangers out there and people are going to take as was just said, you can't control what the bad actors are going to try to do to get access. But I also appreciated the comment that for a manufacturer or a provider they can, having secure information is marketable and should be, they could market it as a premium for the services they are providing and I think we have some businesses here that wrap around this. I think the average individual, we understand having a security office in a corporate setting and probably a sub under the security is data security and obviously, you know, this wireless technology and all these things as a subsection.

So when we hire, when you are looking for a computer programmer to go in cyber, in the cyber world, what is a new engineering computer programmer, what are they going to be doing? I am sure there is a plethora of things, but I mean are they just going to be sitting at a screen watching interactions and trying to pick out and identify an attack? I mean we have all been in, I have been in nuclear, you know, power plants. I have been in data centers. I have been with screens all over the place. Is that what they are doing? Is that what a computer programmer in cybersecurity ends up doing?

Mr. Yoran, do you want to answer that?

Mr. Yoran. I will take a crack at it. In my experience, the best cybersecurity professionals are the ones that just show a tremendous amount of intellectual curiosity in what they are looking at, and sometimes it comes through formal training and discipline and frequently it doesn't. It is usually not the analyst who is sitting behind a screen watching logs go by and trying to pick and choose which one to dig into that is going to make the difference or that is going to scale our industry.

If I could, I think the comment that you made and the Congressman from California are, I won't say two sides of the same coin, but they point to this foundational question of, you know, is there a market failure and what can and should Congress do about it. And from my experience, I think it would be hard to argue that a market, you know, we are not at a point of market failure, everything from, you know, the election to the hack that you see in every newspaper or news distribution point, even real news distribution point on a daily basis.

In order for free markets to work you have to have an educated populous and you have to have a high degree of transparency and I think in the cyber domain we lack that transparency. There is a general lack of appreciation for what the threat environment looks like. There isn't a consistent understanding of what good cybersecurity looks like, what is working in our domain. There

is a lack of transparency when breaches occur outside of ones that impact PII.

And so there isn't a common appreciation for what is not working and also I think what is at stake and what is at risk in using various products. So I think that there is a role for Congress to play around helping to raise awareness and create greater transparency.

Mr. Shimkus. Let me go to just Dr. Clancy real quick because my time is running out. When we travel, which we as Members get a chance to do, we are visiting troops, many times we are asked to leave our computer at home and we are given a little dinky one to be able to continue to communicate. How are we, how secure is the U.S. wireless system versus places else around the world?

Mr. Clancy. I would say the United States has the most secure wireless infrastructure in the world. I think the fact that it -- the things that lead to insecurity in other countries' networks have to do with deployment and use of old technology, a workforce that is managing those networks that is not aware of the latest threats, and the influence of authoritarian regimes over state-owned telecom infrastructure providers in many of those countries.

Mr. Shimkus. Thank you very much. Thank you, Madam Chairman.

Mrs. Blackburn. Ms. Matsui, you are recognized for 5

minutes.

Ms. Matsui. Thank you, Madam Chair, for having this hearing and I thank the witnesses for being here today. Wireless technology and connectedness and of data and information have huge potential to move us forward in a variety of industries.

Ms. Todt, you mentioned in your testimony that you recently had blood work done and were told the only way you could access the results was by downloading an app on your smart phone. I see both potential for good and for danger in this situation. It may be much more convenient for you to receive your test results visually on your phone rather than via snail mail or fax or a phone call. This could result in you acting on that information in a more timely or consistent manner, potentially improving your health.

However, that also means that your data is potentially vulnerable. We saw the risk with the recent malware attacks that brought down hospital systems. Without access to the information that the doctors and nurses relied on to treat their patients they could no longer do so effectively.

Our healthcare system is uniquely at risk of attacks. Most professionals who go into the healthcare field often including administrators don't have a cybersecurity background. We need to work to ensure that our healthcare providers have the technological infrastructure and workforce to manage the complex

data that they need to best serve patients.

Last week, the Department of Health and Human Services released its Healthcare Industry Cybersecurity Task Force Report. Among other things, the report recommended executive education about the importance of cybersecurity. Ms. Todt and any of the other witnesses, what recommendations do you have for developing cybersecurity leadership in industries such as health care?

Ms. Todt. Thank you. I am now convinced given what the chairman said that I was one of the 100 million that got my healthcare records breached last year, but that is something else for me to figure out. I think that what you ask is a great question in relation to also the other questions that have been posed around IoT and workforce, because we tend to think of cybersecurity workforce as those with the engineering degrees.

But what we have to understand in the workforce that we are creating is that everybody has to be educated on cybersecurity. This is not an expertise; it crosses every enterprise. And arguably, I would think that human resources professionals, those who are hiring, have to have a baseline level of knowledge. The other issue is that when you are a manager you have to be trained in cybersecurity so that you know what you are doing regardless of whether or not your function is cyber related.

And I think enterprises need to be looking at cybersecurity education the way, as an onboarding process, the way they look

at ethics and integrity and basic company protocols and procedures. We have to be incorporating cybersecurity awareness and education from the ground up to create this culture and I think that this is something as we move forward to emphasize.

The other issue that this is more of a technical response but we talk about the education of user awareness. From a technology perspective while we are educating the consumers and the individuals and industries and enterprises, we also need to be thinking about moving security away from the end user from an innovation perspective.

Ms. Matsui. Okay. Thank you very much and let me move on to Dr. Clancy. Dr. Clancy, according to one study none of America's top ten computer science programs as ranked the U.S. News and World Report in 2015 required graduates to take one cybersecurity course. Three of the top ten programs didn't offer an elective in cybersecurity.

But with the rise of cyber attacks and security breaches in our networks and the shortage of cybersecurity professionals, it is imperative that our students graduate with the course work needed to be able to tackle security issues. Dr. Clancy, how can Congress encourage our colleges and universities to prepare students either through expanding courses, hiring more faculty, or other innovative solutions for careers in cybersecurity?

Mr. Clancy. So I think the reason you may see that in some

of the top-ranked programs is it is the traditional academic culture that cybersecurity is a buzz word and is a fad, and myself and others in academia are working very hard to convince them otherwise that this is a fundamental problem that is going to be with us indefinitely. I think there are a number of programs that are very positively impacting this ecosystem to include NSA's Centers of Academic Excellence program and the CyberCorps Scholarship for Service program. While the CyberCorps program provides scholarship money for students to pursue careers in government upon graduation like a cyber ROTC program, the funding helps the university establish a platform that can educate students in cybersecurity who go into many different careers, not just into Federal Government. We saw that directly at Virginia Tech as part of our receipt of a CyberCorps grant. I think more initiatives and further investment in programs like that is a great place to start.

Ms. Matsui. Okay, thank you. And I have run out of time, I yield back.

Mrs. Blackburn. Mr. Olson, you are recognized.

Mr. Olson. I thank the chair and welcome to all of our witnesses. Mr. Yoran, thank you, sir, for your service to our country in our United States Army, West Point graduate. Heartfelt congratulations as well, because with assist from Temple for the first time in 15 years your Navy beat my Army in

1283 football. Bravo Zulu.

1284 Your testimony talks about elastic attack surface that
1285 includes a growing number of information technology devices.
1286 Being the vice chairman of the Energy Subcommittee I worry about
1287 cyber attacks on our power grid. December 23rd, 2015, 230,000
1288 people in the Ukraine were without power for 1 to 6 hours, a cyber
1289 attack likely coming from Comrade Putin in Russia. It was very
1290 low tech. They simply remotely flipped some switches.

1291 What kind of advice does your company provide to critical
1292 infrastructure companies in our electric grid regarding how to
1293 best protect their systems for cyber attack?

1294 Mr. Yoran. Thank you, Congressman. I think that is an
1295 ongoing challenge. As early as last night, the US-CERT program
1296 issued additional warning and guidance to energy and critical
1297 infrastructure companies around the Crash Override piece of
1298 malware which is affecting power companies around the world.

1299 From a security perspective there is a great challenge in
1300 that industry in that the systems are incapable of being updated
1301 or there is tremendous risk in updating those systems which,
1302 unlike our mobile phones or desktop PCs, have a life span measured
1303 in decades. From a best practices perspective these
1304 organizations have historically left those critical networks in
1305 the standalone state, but increasingly they are interconnected.

1306 We offer technologies and other companies offer technologies

that help monitor these networks on a passive basis, so without introducing additional risk, additional packets, or probing those networks you can see what they are vulnerable to and you can create a series of compensating controls to protect those systems from internet compromise.

Mr. Olson. Also you brought up artificial intelligence. And as a co-chair of the recently launched Artificial Intelligence Caucus, I believe it is important that we use cybersecurity technology to complement the work of the talented human brains that make this happen.

We know that technology alone won't solve the cybersecurity issues we have, but can you elaborate on how leveraging this technology for the growing AI field will work do you think, cybersecurity in the AI field -- or Mr. Wright, Dr. Clancy, Ms. Todt? Somebody want to take that? It is not bomb, not a grenade.

Mr. Clancy. I am happy to take a stab at that, I think the DARPA Cyber Grand Challenge that we saw last year is an example of a first step in being able to accomplish that. As I mentioned earlier, I think that AI will become initially a tool that helps analysts do their job more effectively and more scalably to deal with the growing threat and larger and larger amounts of data.

There is an AI renaissance that is happening, right. There are fundamental advancements that are happening that are completely changing the world of image processing and search that

Google and others are leading. And I think there are many in the cybersecurity community that are hoping that those technologies can be applied to the cyber problem, but that is still an early research area that many people are sort of feverishly working on right now in academia.

Mr. Olson. Ms. Todt, you look like you are chomping at the bit to comment. Am I reading that wrong?

Ms. Todt. Just in support I think that we need to be investing obviously in innovation. I was on a panel with somebody who used to work at DARPA who essentially talked about the fact that there are functions that really aren't meant for humans and that our ability to automate and make those functions more capable through super-computing will help our systems work more effectively.

Mr. Olson. One final question for you, Mr. Yoran. We are seeing an explosion of free WiFi hotspots all around the country, whether they are there at the corner coffeehouse, the Starbucks, the airport, the airplanes you mentioned; heck, the Mr. Carwash right down the street from my house. My daughter and wife go there all the time. It has a free hotspot just for the 20 minutes you are there.

Do they offer unique challenges to safeguard? If so, what should be done on the network side as opposed to the user side?

Mr. Yoran. Well, I think the most important thing is to

recognize that whether you are going to a public hotspot or you get fooled into connecting to a rogue hotspot or you are connected to a corporate network which is already compromised and frequently is, the most important thing that you can do and that organizations can do is better assess the vulnerability and exposure of their systems and make sure that they are applying the latest patches and they don't fall victim. A vast majority of the attacks that we see come from well-known, well established vulnerabilities to which patches are readily available.

Mr. Olson. Good luck, Army. I yield back.

Mrs. Blackburn. Mrs. Dingell, you are recognized.

Mrs. Dingell. Thank you, Madam Chair, and thank you for doing this hearing and to all of the witnesses. There are so many questions. Cybersecurity is something that should concern all of us. And as somebody who has been hacked more than anybody would want to be I can tell you it is a pain to have to change your password and switch to two-factor authentication and worry about personal information being compromised.

I think what -- and not even what I prepared -- what is really worrying me is some of the factoids that you have raised here today. I think one of the issues is training people. Even when you have trained IT people and you go to them and you ask a question -- ask John Podesta, myself have done this -- should I do this? And they say oh yes, and then it turns out not to be the right

thing. I think I got one last night that I have now been burnt so much I was smart enough to wait and talk to somebody today.

And I really worry about as we start to talk about autonomous vehicles as an example, if people don't -- how are we going to make sure patches that need to occur occur, and when they don't, even when we look at the health care what happened on the health care situation there were simple patches available that users aren't using. How do you legislate that? These are real issues.

But for these 5 minutes, which are now down to 3 minutes and 45 seconds, let's talk about mobile phones which as you said, Mr. Wright, are basically super computers we have in our pockets. Our phones are always by our sides. We store our most intimate and personal details in them. And it is happening now and in the near future people are going to be locked out of their phones and in turn will be locked out of personal, social, financial information. That is a new experience for everyone. We are going to see this high level of hysteria, and we have got to pay attention to it.

So this question is for the entire panel. Ransomware is now available as a service making it incredibly easy for criminals to carry out an attack. What can government do from a policy perspective to increase barriers to entry and the cost of carrying out ransomware attacks, and do you think the threat of a ransomware attack on a mobile device will only continue to increase if the

government doesn't do something, any of the panel?

Mr. Wright. I can start out here. Starting with your last question I think that mobile ransomware will probably increase no matter what is done. Again the criminals follow the money and right now your handheld computer is where that money or where that data is. When they can figure out how to monetize locking up that phone or encrypting that data on your phone enough to the point where you will pay to get it back, then in that case mostly not get the data back, they will exploit that.

Mr. Yoran. I don't think any of us are comfortable with the state of security on mobile phones, but I think a lot of progress has been made. A lot of lessons have been learned in the -- some have not, but a lot of lessons have been learned in the mobile domain from decades of mistakes and accidents in operating systems and in compute platforms from the desktop paradigm.

So I am confident that we will see an increase in ransomware no matter what is done on mobile platforms given how attractive they are as a target, but I think the industry is making progress to make that more and more challenging over time.

Mr. Clancy. I think that if you look at ransomware it is leveraging the same vulnerabilities that people have used to exploit mobile devices for the last decade. So continued work to make sure patches are deployed and apps are updated is critical to closing the front door, if you will, to ransomware.

I think other areas that are somewhat unique to ransomware have to do with educating users about the importance of backing up their data so if they are a victim of ransomware attack they are able to recover their data. Many cellular providers offer free services to back up your data on your phone to the cloud and consumers need to take advantage of that.

Secondly, I think there is really the forensic and law enforcement side of being able to follow the money and be able to take down the ransomware networks which is increasingly difficult with the rise of bitcoin and other crypto currencies, but that is perhaps a larger question.

Ms. Todt. I think ransomware represents sometimes a little bit of the flavor of the day in that we have these problems that continue to evolve, but the solutions for them are the same when we look at WannaCry which was, you know, essentially not updating with patches that are there. So it is a lot of the cyber hygiene that we have talked about and the regular download.

I think it is also important, you raise an interesting element to this which it is often important to remember that attacks and when data is compromised or manipulated it is not usually because there is some engineering expertise or genius, it is really about opportunism and being able to access and exploit that opportunism. And so that is why education, backing up, all of those very basic actions can really cover about 80 percent of

the solution.

Mrs. Dingell. I had more questions, but I am out of time. Thank you, Madam Chair.

Mrs. Blackburn. And we will give the opportunity to submit those questions in writing. Mr. Johnson, you are recognized 5 minute.

Mr. Johnson. Thank you, Madam Chairman.

Mr. Yoran, in your testimony you note that there is a shortage of skilled labor in the cybersecurity workforce. How acute is that shortage? Has it manifested itself in your company? Do you have a problem hiring those kind of people in your own business?

Mr. Yoran. That is a great question. It is extremely competitive to hire experienced cybersecurity professionals. The compensation is great and as they continue to gain experience, you know, their expectations continue to rise.

Mr. Johnson. On the technical or the strategic side, because I mean there is a big difference between people that understand what cybersecurity is and those people that can get down to the ones and zeros and kind of do the technical wherewithal to find out who the bad guys are.

Mr. Yoran. I think there is really a shortage on both fronts, which is why I think the importance of Dr. Clancy's comments around the multidisciplinary approach to cybersecurity. What we found is in addition to compensation there is two other

critical aspects to attracting and retaining cybersecurity talent. One is in providing them intellectually stimulating work. It is an exciting field and if you don't give them exciting problems they will go elsewhere to find them. And the other is in creating a culture that is dynamic and one that is enjoyable to be part of.

Mr. Johnson. Okay. Do you think we have the same level of expertise shortage in finding skilled workforce in government agencies or departments? Is it worse, the same?

Mr. Yoran. I don't know that I have the data in front of me to comment whether it is worse or the same. I do know that a tremendous amount of expertise in the private sector starts out getting its experience in public service which is costly to the government in terms of losing that talent, but I think it provides tremendous value to the private sector in terms of the level of maturity and understanding of very sophisticated cyber threats.

Mr. Johnson. Okay, all right. Thank you.

Dr. Clancy, what a name for a topic like cybersecurity. And if your first name was Tom you would be --

Mr. Clancy. It actually is.

Mr. Johnson. Yeah. I would consider changing it if I were you.

Mr. Clancy. No, no, seriously, my name is Tom Clancy.

Mr. Johnson. Okay, all right. Will the real Tom Clancy

please stand up?

Mr. Clancy. I go by my middle name Charles. It causes too much confusion.

Mr. Johnson. Well, Dr. Clancy, how soon should we expect biometric tools to supplant the traditional pin and password approach to device security?

Mr. Clancy. So biometrics have offered a tremendous opportunity to fundamentally change how we authenticate people. I think there are still challenges. The joke in the biometrics community is that if I am using a fingerprint as my password I can only change my password nine times before I run out of fingers.

So there are some challenges there. If your fingerprint data is compromised because it is stored in a database then your credential is sort of irrevocably lost and you can't change it like you can change a password.

Mr. Johnson. So in that regard then, in that vein do you think biometric tools are going to make us more secure or are we going to happen upon the same kinds of problems that we have now if we file them away?

Mr. Clancy. I believe that biometrics will be a critical part of multifactor authentication. If combined with a password and a mobile device, right, you can fuse these things together in order to significantly improve the security of a particular authentication to some online service.

Mr. Johnson. All right. Secondary question, do you think it is right to think of every connected device as a potential vulnerability and, if so, what freedom or flexibility should network operators have to promote security when device owners fail to do so? And I guess we are sort of getting into the Internet of Things, you know.

Mr. Clancy. Certainly. So the internet service providers have an increasingly challenging time. Because of the rise of technologies like end-to-end encryption, it is very difficult for internet service providers to tell the difference between a botnet command and control packet or a standard IoT web service traffic just because they don't have the visibility that they would otherwise have.

So I think that that creates problems for them that makes it a challenge for the entire ecosystem, where you need the IoT service providers and the device manufacturers and all of them to come together to come up with a common solution for securing IoT.

Mr. Johnson. Okay. Ms. Todt, I apologize. I had a question for you but I have run out of time. Madam Chair, I yield back.

Mrs. Blackburn. Well, we will also let you submit that question in writing. Okay, Ms. Clarke, you are recognized for 5 minutes.

Ms. Clarke. Well, thank you, Madam Chair. The FCC just announced the newest members of the Communications Security, Reliability and Interoperability Council, a council established to make recommendations about the security, reliability, and resiliency of our communications systems. But as I have reviewed the names of the new members, I am disappointed to see a lack of cybersecurity expertise on the council.

As the author of the Cybersecurity Responsibility Act, my bill makes it clear that the FCC has a role in ensuring our commercial sector has protections in place to secure our communication networks from malicious cyber attacks. So Ms. Todt, what role do you believe the Federal Government, in particular the FCC, has in protecting our nation's communication networks?

Ms. Todt. Well, I think again we can look to the executive order that was released by President Trump in May which specifically calls out the FCC as having a role in protecting the communications infrastructure and working with the secretary of commerce and the secretary of the Department of Homeland Security to initially look at that botnet mitigation, but then also looking at clean pipes and where that goes. And so clearly, I think the government, the executive office as well as industry, believes that there is a role that it needs to play.

Ms. Clarke. So then it would be prudent to have some

cybersecurity expertise on this council, wouldn't it?

Ms. Todt. That would appear to be the case, absolutely. I don't know who those individuals are so I don't know if they have them in any --

Ms. Clarke. Just generally speaking.

Ms. Todt. But I would say, I mean this is the issue, the broader issue, is that we have to be bringing cybersecurity expertise into all of these areas and that we have to be looking for that because that knowledge and that expertise has to be informing our policies, because they don't even have to be cybersecurity policies but they have an impact.

Ms. Clarke. Absolutely, thank you.

Dr. Clancy, as part of Congress' resolution of disapproval that overturned the FCC's privacy protections, Congress also stripped away consumers' data security protections. As I noted before, my bill, the Cybersecurity Responsibility Act, would ask the FCC to take some action, any action to protect our networks. Did Congress' rollback of these data security rules do anything to make America's personal information more secure?

Mr. Clancy. Well, I --

Ms. Clarke. Use your mike.

Mr. Clancy. So I think the rollback of the cybersecurity provisions in the FCC rulemaking from 2018 was, actually happened before Congress acted, right. The FCC removed those provisions

and stayed those portions of the regulation, and then ultimately Congress rescinded the entire order which was focused more on the privacy aspects of that rulemaking.

Of course the state of rationale was that it was inconsistent with the Federal Trade Commission's view of privacy and opt-in versus opt-out when it comes to consumer privacy. I don't know that I am in a position to declare whether opt-in or opt-out is a more appropriate way to protect consumer privacy, but I think it represents some of the regulatory challenges we have in asserting that one particular regulator has authority over a very complex ecosystem.

Ms. Clarke. Or the question was more about security. And just looking at the ecosystem, if you sort of strip those or rollback those security rules, we are trying to figure out whether people's personal information it becomes, did we open up vulnerabilities? Let's put it that way.

Mr. Clancy. So based on my experience working with the cellular industry and some of the major internet service providers, the big companies are already doing those best practices. The large ISPs, the large wireless carriers are already doing that. Where the gap is is the smaller and more rural internet service providers and the more niche wireless carriers who don't have as much infrastructure or resources themselves to deploy those best practices.

Ms. Clarke. Yeah. So when there is a vulnerability even in the smallest of these providers, doesn't that open up opportunities to get at grander --

Mr. Clancy. Certainly, it does given the interconnectedness of the different telecom providers. I think what we are seeing in industry is strong collaboration though, with the big guys looking out for the small guys and doing what they can to help quickly remediate through information sharing that was really accelerated by the past --

Ms. Clarke. Anyone else have any thoughts on that?

Ms. Todt. I think the supply chain is a huge issue and even if you are sharing those practices we have to be looking at baseline level of standards. And I think that you are, oh, it is always going to be the weakest link and we have to do a better job within our sectors of actually informing and helping to share those best practices and lessons learned. One of the things that we have learned is that small businesses across sector have a lot more in common with each other than the small businesses and the large businesses within their sector and there is a lot of evidence right now around that. And so being able to look at this more thoughtfully and I think it goes again to this issue of collaboration and pre-event planning would be the actions that we need to be taking.

Ms. Clarke. Very well. Madam Chair, I yield back. Thank

you.

Mrs. Blackburn. And Mr. Bilirakis, you are recognized for 5 minutes.

Mr. Bilirakis. Thank you, Madam Chair. I appreciate it so much. And I appreciate your testimony today.

As more IoT devices enter the market industry has seen a rise in tech support scams, unfortunately. Symantec's 2016 Threat Report found a 200 percent rise in tech support scams in a 2-year period. With these types of threats the best defense is with the end user. Mr. Wright, how can an end user distinguish between a legitimate help desk and a tech support scam and can you describe how Symantec has responded to the increased threat?

Mr. Wright. Yes. So these types of social engineering attacks as you just mentioned the tech support are particularly vexing. They depend on the consumer to somehow be able to intuit or to understand whether or not they are being, whether they are being scammed. There is not a lot of sort of technology that can fix that. A lot of it comes back to raising awareness of the user of what those threats could be, those users being more careful and perhaps having a more keen eye on to pick up signs. But it is a very, very difficult problem when it comes down to the user themselves.

Mr. Bilirakis. Yeah, thank you. For years people have been told to check for the https identifier in their browser before

accessing personal websites such as for banking or health care. Mr. Wright again, your 2016 Threat Report states that relying on the https marking provides a false sense of security. Can you expand upon that?

Mr. Wright. I am sorry?

Mr. Bilirakis. Your findings. No, let me say it again. Your 2016 Threat Report states that relying on the https marking provides a false sense of security. Can you expand on that finding?

Mr. Wright. I know that https is more protected, but I am sorry I cannot sort of expand on the Internet Security Threat Report piece there. I am not prepared for that. Anybody on the panel have --

Mr. Bilirakis. Okay. Can maybe anyone else on the panel? Yes, please.

Mr. Clancy. So https implies that the session is authenticated and encrypted, but the concern is to whom you are authenticated. There are many scams that can change a letter in the name of the domain name such that you wouldn't notice the difference but could still present a secure credential to you as a user.

So I think https is a first step and if you don't have that then you definitely need to be concerned. But there are other -- you need to look at the spelling of the domain name to make

sure that it is spelled accurately and there aren't strange characters in there, that those are the sorts of things that undermine the security of simply looking for the https.

Mr. Bilirakis. Any other suggestions?

Okay, thank you very much. Let's see, I still have a little time. Mr. Wright, according to Symantec 2016 Threat Report, the Apple iOS system faced its first widespread threat with the XcodeGhost attack. This malware has infected over 4,000 apps which leaves unsuspecting devices vulnerable. In response to cyber threats success largely depends on speed of response. How has industry responded to threats via apps since it first took hold in 2015 and have efforts met the success?

Mr. Wright. Yeah, good question. So apps certainly represent a potential threat vector especially for mobile devices. I would say that Apple has done a pretty good job making sure that malicious apps are not included in their app store. Android is doing a better job at trying to ensure that their apps aren't malicious. So those two providers I think have come a long way. Apple has always been pretty good, but the other provider has come a long way.

In addition, there is some security solutions to this. Not plugging Symantec, but we do produce technology that can scan for apps and look for possible malicious apps or grayware apps which sometimes can leak information. So there is a technology

solution, and then also the providers are doing a lot of work in that area as well.

Mr. Bilirakis. Anyone else want to add something? I know I only have 15 seconds. Okay, very good. Thank you, Madam Chair. It is a very informative hearing. Thanks for calling the hearing. Thank you.

Mrs. Blackburn. Thank you. Ms. Eshoo, 5 minutes.

Ms. Eshoo. I thank the chairwoman and I thank all the witnesses. I think you have given very important testimony. First of all, to Mr. Wright, I am very proud to represent Symantec.

Mr. Wright. Thank you.

Ms. Eshoo. I have had a long, long, long-term relationship going back to the days of John and how he really helped build a new Symantec and you keep going and you are a real asset to the country.

And to Mr. Yoran, you get the prize for the best dressed before this subcommittee every time you come. One of the members said, do you think he lost his suitcase? I said, no, he hasn't lost his suitcase. That is his tuxedo for this committee.

You have all -- there has been a lot of discussion about a lot of things here. The title of the hearing is Cybersecurity Risks to Wireless Networks, but this is an entire ecosystem. And I think we have made real progress in many areas and I think that obviously we are lacking in others. I want to thank Symantec for

working with me on the legislation that I mentioned in my brief opening statement. But I want to go to something else first and then a question to each one of you. Last year the FCC put into place data security rules that apply to wireless carriers as part of its privacy proceeding. And Dr. Clancy, you just gave some kind of, I don't know really what it was, but I am going to find out more, press you for more.

These rules asked ISPs, really, something very simple and that is to take, quote, reasonable measures, reasonable measures to protect consumer data. Now there was the monetization of information and the monetization of attacks that has been brought up by more than one panel member this morning. Do any of you think that the FCC went too far in asking ISPs to act reasonably to protect consumer data? There is a little bit of, if I might suggest this, politically cross-dressing that is going on here, because the Congress ripped away all privacy protections on the internet and that is on the computer that I have in my purse. That is for everyone in the country. So we are talking about, I think cybersecurity is all about privacy. It brings about privacy.

So maybe a yes or no to each one of you, and if you don't know then say that. Do you think the FCC went too far in asking for reasonable measures to protect consumer data? I am going to start with --

Mr. Wright. So I will have to say I don't know too much about

that --

Ms. Eshoo. Okay.

Mr. Wright. -- specifically, but I will say, you know, it appears to be reasonable to protect user data.

Mr. Yoran. I can't comment specifically to FCC's issue, but reasonable does sound reasonable.

Mr. Clancy. Indeed. I mean it was a complicated set of circumstances, but --

Ms. Eshoo. What is so complicated about it? What is complicated about it? I have it right here what they put forward. They are really simple things.

Mr. Clancy. Reasonable is reasonable.

Ms. Todt. I will ditto my colleagues. I mean reasonable protections are reasonable.

Ms. Eshoo. I think what I would like to do in writing, because I don't have time for it, is to ask each one of you so you can be prepared for it, what is your top line recommendation to the subcommittee relative to cybersecurity in our country? Just one thing, top line, from each one of you. You are all experts and I will look forward to sending that to you and getting your responses. Thank you for what you are doing for the American people. I appreciate it.

Mrs. Blackburn. All right. Let's see, we are -- Mr. Flores, you are recognized.

Mr. Flores. Thank you, Madam Chair, and I want to thank the panel for being here today.

Ms. Todt, unlike other types of crimes, when we talk about cybercrime we always seem to focus on the need to protect against the attacks rather than prosecute the bad actors. And can you tell us what the Federal Government is doing to actively work on cybercrime attribution and also what are the limitations of trying to track down our cyber adversaries?

Ms. Todt. So right now I believe the executive order has laid out -- I am not as familiar with the criminal angle. I know we worked with the Department of Justice with the Commission on being able to look at malicious actors and where the crime plays a role, and I think one of the key things that a lot of the commissioners talked about is you have to have penalties for those bad actors. But I apologize, I can't talk extensively, but I am happy to get back to you with an answer in writing.

Mr. Flores. Okay, yeah. If you could do that, that would be great.

Dr. Clancy, in your testimony today and from testimony across the panel it sounds like we have got a skills gap when it comes to protecting ourselves from cybercrime. And of course in order to fill the pipeline we are going to have to be able to get our educational institutions to produce the people resources to be able to do with this.

I represent three world-class universities back in my district, Texas A&M University, Baylor University, and the University of Texas. What could the Federal Government be doing to help ensure that pipeline is filled with quality skilled individuals?

Mr. Clancy. I think that most of the efforts to date have focused on the tail end of the pipeline.

Mr. Flores. Right.

Mr. Clancy. Getting students out of college and into jobs, I think the pipeline starts much earlier than that.

Mr. Flores. Exactly.

Mr. Clancy. When students are coming into college they need to want to major in cybersecurity and more broadly in STEM fields, so I think additional initiatives that are focused on the K-12 outreach and engagement to bring cybersecurity down to the middle school level or even sooner, just basic digital hygiene at the elementary school level would be a great starting point and build up from there. If you want to build a pipeline you need to start at the beginning.

Mr. Flores. Okay. Now Mr. Yoran, you and I both have business backgrounds and I mean you hire a lot of these types of individuals. What would your key recommendations be?

Mr. Yoran. I think it is important for employers to look for the intellectual curiosity around cyber. And as Dr. Clancy

said earlier, you know, I think you have to start at an earlier age and part of it may be through cyber hygiene. I know I could talk to my kids about cyber hygiene and they still don't apply their patches, so I think we have to find things that are more interesting, more intriguing ways of creating excitement and creativity around cybersecurity education.

Mr. Flores. Okay, thank you.

Dr. Clancy, you mentioned the need for the Federal Government to continue to act as a convener and to set priorities based on its unique knowledge of cyber threats, but for national security reasons the government doesn't always share the full extent of its knowledge of those threats. How significant is this limitation and how can Congress be helpful in encouraging more transparent threat intelligence sharing?

Mr. Clancy. So I think from a convening perspective, groups like the FCC CSRIC organization is a great way for the government, for the Federal Communications Commission to sort of set priorities and identify areas of concern and work collaboratively with industry to identify solutions. I think that that goes to a certain extent hand in hand with the challenges of cyber information sharing.

You have the national security agencies who are generating detailed information on cyber threat, but that is due to the sources and methods involved. It is held at a classified level

and can't be shared and that creates a barrier to sharing. The thought is that if we have sufficiently large cyber threat brokerage houses sort of emerging that there can be enough data that the Federal Government could anonymously share data that would obscure sources and methods with those brokerages and it wouldn't be attributable to specific sensitive aspects of how that data was arrived at.

Now we are not there yet, but I think there is some hope that that may be a solution moving forward long term.

Mr. Flores. Okay, thank you. If any of you have any supplemental comments on any of these questions and you could submit those that would be great. Thank you and I yield back the balance of my time.

Mrs. Blackburn. Mr. Rush, you are recognized for 5 minutes.

Mr. Rush. I want to thank you, Madam Chair, and I want to commend you for holding this hearing.

Dr. Clancy, Tom, you are concerned that the Internet of Things, the IoT, where everything from home appliance to industrial infrastructure devices connected to the internet is not secure enough to withstand a cyber attack. What is the biggest challenge you see in securing this complex mobile ecosystem?

Mr. Clancy. Well, I think that just the breadth as you stated is part of the challenge. The threats to an

internet-connected home appliance are very different than the threats to an internet-connected nuclear reactor and the technologies involved are very different.

So at one end of the spectrum in the consumer technology space we have the key challenge, I think, is supply chain and inexpensive goods, inexpensive IoT devices coming from overseas that were not designed with security as part of the fundamental component. I think at the other end of the spectrum you have industrial infrastructure, industrial control systems. There the challenge is more that the desire to gain efficiencies from aging infrastructure and be able to support more users with the same power grid and more peak demand requires us to use artificial intelligence to orchestrate much of our infrastructure which necessitates connecting that infrastructure to the cloud in order to do the needed big data processing on the data.

So you end up drawing this sort of series of events that necessitates for business reasons connecting this industrial infrastructure to the cloud, which then fundamentally exposes it to risks it had never faced before. And that is a whole separate set of challenges that requires the key components of that industry to figure out how to work together to solve those challenges.

Mr. Rush. Are you concerned that the Federal Government is inadequate and then presently is organized that we are, are we

prepared to deal with this broad threat, a cybersecurity threat? I mean we have different centers of responsibility or authority and power located in many different places from Homeland Security to the FCC. Are we prepared in a streamlined way to respond to a cyber attack using these IoTs?

Mr. Clancy. I think we are never going to be as prepared as we would like to be, but I think our level of preparedness is steadily increasing. I think the NIST Cybersecurity Framework that many have referenced throughout this hearing is a great example of a tool that we can use to develop a common understanding of how to respond to these threats and we need more things like that to help improve our ability to respond.

Mr. Rush. I want to thank you. I want to move to Mr. Wright. Mr. Wright, how vulnerable is the U.S. power grid to a similar power grid attack that Ukraine suffered last year?

Mr. Wright. Excuse me. Yes, you are referring to what we have called Sandworm threat. It attacked the Ukraine two different times over the last year shutting down power. Interestingly, they got back online relatively fast because they went back to manual movements.

Here in the U.S. I think we are probably more advanced on our security of those power grids. More than that, I think that our people are trained to be able to get back online manually because of threats in storms and natural disasters that they have

trained to be able to get back online and to be able to do that manually.

That said, there is always going to be susceptibility, and with the latest Ellen Nakashima article that came out yesterday advising of a new more advanced threat, I am sure that our power grid operators and government are looking at how to protect against those.

Mr. Rush. I want to thank you, Madam Chair, and I yield back.

Mrs. Blackburn. I thank the gentleman. Mrs. Brooks, you are recognized for 5 minutes.

Mrs. Brooks. Thank you, Madam Chairman, and thank you to all of our panelists for sharing your background and your wisdom with us. It seems that part of the problem we face is that cyber attacks when we talk about cybersecurity it is moving far faster, it seems, than our cyber defenses and the bad guys only have to be right once while the good guys have to be right all of the time.

I am a former U.S. attorney and but from '01 to '07 when we were really standing up cyber teams and I certainly know the FBI and obviously NSA and others have really beefed up their cybersecurity, but yet I am a bit troubled that -- because I was just, you know, Googling big cyber cases and so forth and they seem to be happening more in other countries than they are happening in our country.

And I am just curious how much cooperation is there with the

private sector lending your advice to the government sector in prosecuting and enforcing our cyber laws. And I am concerned that your expertise and the expertise of those in your industry, it is hard for government to bring folks in. As you said, I believe, Mr. Yoran that often it goes the other way. They start in government and then go out to the private sector.

But yet if we aren't cooperating and I think at a very different level than we currently are, and I appreciate your work and what the commissions have done and recommendations and so forth, but I think we need to accelerate it in a much greater way of how we can prevent, not just prevent because you are all focused on preventing, but if we don't actually prosecute. And Mr. Wright, would you like to start us out?

Mr. Wright. Sure.

Mrs. Brooks. And I really need to hear what your thoughts are about the level of government's willingness to bring your expertise to the table to help us, you know, stop these people by actually prosecuting.

Mr. Wright. Yeah, I think you are making an absolute, excellent point there. There is a focus on protection, whereas rarely do we speak about deterrents. One of the main deterrents is prosecuting. I would say that the FBI in particular has gotten much better. In fact, I would put them at very good at this point. They are recruiting the right people. They are going after the

cybercriminals. And maybe if you don't read about it as much here in the United States it is because a lot of our adversaries, cybercrime adversaries, are sitting overseas; very tough to prosecute in those cases.

But I will tell you one good story that happened right at the beginning of this year. Symantec partnered with the FBI and worked on a case we referred to as Bayrob. It went on for 9 years. We had finally culminated in the arrest and extradition of three Romanian citizens that are currently sitting here in the U.S. awaiting trial.

Those connections that private sector companies are making with law enforcement are getting better every day. They are getting more and more trusted. I actually think that is a good news story for us now. But I think focusing on some sort of deterrents is really important because today cybercrime has all upside and no downside. There are no risks, very few risks involved in being in cybercrime.

Mrs. Brooks. Thank you. Mr. Yoran, any comments you might have and should we be looking at a different model of how government is working with the private sector to bring people to justice? Because 9 years and three defendants doesn't sound like enough to me, but I applaud it -- but 9 years and three defendants.

Mr. Yoran. And I am sure there is a lot of detail to that case and will point to many follow-on cases and other

investigations. I think you bring up a very important point. There are many cooperative efforts between law enforcement and private industry.

A few areas where private industry has really augmented what has been traditional government function is in the area of attack attribution and threat intelligence of which Symantec, you know, is a very active participant. And that can aid and assist law enforcement and also help create deterrents whether it is through naming and shaming or other means.

There also remains, I think, a reasonable gap between the interest of law enforcement and those trying to defend networks where there are instances where, you know, law enforcement officials would like to, for the purposes of prosecuting a crime, leave systems open and to continue to monitor how a crime is unfolding, whereas those trying to defend networks frequently care a little bit less about who is doing it and more about cleaning up their systems.

Mrs. Brooks. My time is up, but if any of you would have any other comments you would like to make, would certainly appreciate any written comments on it. Thank you. I yield back.

Mrs. Blackburn. Thank you, gentlelady, and Mr. Costello for 5 minutes.

Mr. Costello. Thank you. Mr. Wright, from your experience working on both the federal side and industry sides of

cybersecurity, I want to ask you this question. And this comes from a conversation I had with somebody pretty high up the food chain on this issue. Mobile device hardware, how serious of a problem is it that DOD and the U.S. Government rely on foreign IT hardware as well as just the consumer products that we utilize in that space? Many of it is foreign manufactured or foreign designed and specifically I have heard that there are times when the capacity or capability of a particular device far exceeds, the potential for it far exceeds what the realization of that device is actually for. Does that make sense?

Mr. Wright. So I think the capacity and capability --

Mr. Costello. In other words you can have more with --

Mr. Wright. Far exceeds, I am sorry? What --

Mr. Costello. Far exceeds what a consumer is actually intending to utilize it for.

Mr. Wright. Well, I think that certainly on this side, mobile phone consumers are sort of just hitting the beginning of what they eventually are going to do with mobile devices. As far as concern about where those mobile devices are being built, you know, I think that some of these supply chains are always going to be important and can open up some possible vulnerabilities.

So we need to be able to have an understanding of where not only the device is put together but where those individual pieces are manufactured and pulled into the device, because they can

certainly open yourself up to vulnerabilities.

Mr. Costello. I want to pick up on the line of inquiry that Mrs. Brooks was pursuing and that is, it seems to me distinguishing between lawful legitimate activity and unlawful activity, someone engaged in a cybersecurity crime is often difficult to discern until it is too late. And whether it is the cloud, whether it is wireless access points, I was reading a little bit in the testimony about the mobile device management solutions.

The question I have here is, is our criminal code, does it reflect the technological capacity of cybercrime as it stands today or are we sort of, is it antiquated? Does it need to evolve or does it need to be, does it need to reflect the way that criminal activity occurs, because often times a crime could be happening and yet we are not able to call it a crime because the actual malware or the actual money hasn't been stolen or the last piece of the crime which would actually make it criminal hasn't yet occurred. Does that make sense?

And so my question to any of you is, be it with wireless access points, be it with just how often we use the cloud, do you see certain types of cybercriminal activity where our criminal code does not properly reflect what is happening day in and day out in such a manner that we are able to go and prevent crimes from happening because our criminal code does not have the elements to be able to have us sufficiently charge them with a crime early

enough before it is too late, anyone?

Ms. Todt. I think the industry, obviously industry has a thoughtful perspective on this and I know Symantec has done some tremendous work in this space. There is an entity called the National Cyber-Forensics & Training Alliance center which works with the FBI with consumers with law enforcement to understand where the criminal code is aligned with cybercrime.

And I know that they are working on revising it where necessary, because I think, you know, to the point that was made, rightly, it is this deterrents effort. But updating just as we need to do across all elements of cybersecurity we tend to have a physical approach to cybercrime sometimes and understanding that the NCFTA, I believe, is looking at that specifically.

Mr. Costello. Yeah.

Mr. Wright. I would just say, yeah, I agree there are some sort of unique things about pursuing and prosecuting a cyber case, chain of custody of evidence is one of them.

Mr. Costello. Right.

Mr. Wright. I can't think of sort of specific incidences where we are crosswise with the laws, but that is certainly something I think they could look into. There is one area, the way that we share information, prosecutorial information with other countries, our MLAT process, our Mutual Legal Assistance Treaties, I believe are outdated. They need to be, they probably

need to be revised so that we can share information, we could have information shared with us so that we can prosecute better.

Mr. Costello. The concern I have, and my time is over, is just given the lack or small number of instances where we are able to prosecute on this tells me that there is just too much, there is no risk. I think that was the term you used. There is no risk to not engage in cybersecurity crimes when you are these actors. And that is terribly concerning and it just raises the question to me on the criminal side of it, is there more that we can do to enable the prosecution of this more easily. I yield back.

Mrs. Blackburn. The gentleman yields back and there are no further members seeking time for questions. Pursuant to committee rules, I remind members that they have 10 business days to submit additional questions.

And I think you all are probably aware you have got written questions coming to you. We would ask that you respond to those written questions within 10 business days and get that back to us. It is a hearing where there is a good bit of interest and we look forward to moving forward on this issue this year.

So seeing no further business to come to the subcommittee today, the committee is adjourned.

[Whereupon, at 12:04 p.m., the subcommittee was adjourned.]