This is an unedited transcript. The statements within may be inaccurate, incomplete, or misattributed to the speaker.

RPTR MOLNAR

EDTR SECKMAN

SAFEGUARDING AMERICANS' COMMUNICATIONS:

STRENGTHENING CYBERSECURITY IN THE DIGITAL ERA

THURSDAY, JANUARY 11, 2024

House of Representatives,

Subcommittee on Communications

and Technology,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to notice, at 10:02 a.m., in Room 2123, Rayburn House Office Building, Hon. Bob Latta [chairman of the subcommittee] presiding.

Present: Representatives Latta, Carter, Bilirakis, Walberg, Dunn, Joyce, Weber, Allen, Balderson, Fulcher, Pfluger, Harshbarger, Cammack, Obernolte, Rodgers (ex officio), Matsui, Clarke, Veasey, Soto, Eshoo, Cardenas, Craig, Fletcher, Dingell, Kuster, and Pallone (ex officio).

Staff Present: Kate Arey, Digital Director; Nick Crocker, Senior Advisor and Director of Coalitions; Sydney Greene, Director of Operations; Slate Herman Counsel; Tara

Hupman, Chief Counsel; Noah Jackson, Clerk; Daniel Kelly, Press Assistant; Patrick Kelly, Staff Assistant; Sean Kelly, Press Secretary; Peter Kielty, General Counsel; Emily King, Member Services Director; Giulia Leganski, Professional Staff Member; Brannon Rains, Professional Staff Member; Michael Taggart, Policy Director; Hannah Anton, Minority Policy Analyst; Keegan Cardman, Minority Staff Assistant; Waverly Gordon, Minority Deputy Staff Director and General Counsel; Tiffany Guarascio, Minority Staff Director; Dan Miller, Minority Professional Staff Member; Michael Scurato, Minority FCC Detailee; Andrew Souvall, Minority Director of Communications, Outreach and Member Services; and Johanna Thomas, Minority Counsel.

Mr. Latta. Well, good morning. The subcommittee will come to order, and the chair recognizes himself for an opening statement. And, again, welcome to the Communications and Technology Subcommittee's first hearing of 2024.

The telecommunications industry stands as the backbone of our interconnected world, facilitating seamless communication and driving the digital economy.

But with increased connectivity comes a growing threat landscape that demands vigilant cybersecurity measures to defend against malicious actors and ensure the resilience of our telecommunications infrastructure.

Astonishingly, every 39 seconds, a cyber attack occurs, underscoring the relentless nature of the challenges we face in safeguarding our digital infrastructure.

Industry faces evolving cyber threats, ranging from general, brute-force attacks to sophisticated and targeted deception. Common threats include distributed denial-of-service attacks, which disrupt service availability by overwhelming networks with traffic; phishing attacks targeting users to compromise sensitive information; and ransom attacks, which paralyze operations and hold critical data, like patient health information, captive.

Additionally, the rise of the Internet of Things, IoT, devices allows us to be more connected to our surroundings more than ever before. From smart home appliances to wearable gadgets, IoT devices have transformed the ways we live and work.

However, their proliferation creates new and complex cybersecurity challenges that need careful consideration and robust solutions.

With billions of interconnected devices, each with its own set of vulnerabilities, the possibility of attacks expands exponentially.

To combat these threats, the Federal Communications Commission, FCC, announced the creation of a voluntary cybersecurity labeling program for smart IoT devices with the goal of protecting American users. This program, called the U.S. Cyber Trust Mark, would place a logo on products that meet a basic level of security.

The security requirements would be developed by the FCC and based heavily on the work of the National Institute of Standards and Technology, NIST.

While I still have a few questions regarding the voluntary nature of this program, particularly in light the FCC's recent net neutrality and digital discrimination orders, I am pleased that the Commission is taking proactive steps to protect Americans from cyber attacks.

As we navigate the complex landscape of cybersecurity, collaboration between industry, stakeholders, government agencies, and cybersecurity community is paramount.

Developing and sharing best practices, threat intelligence, and technological innovations will strengthen our collective defenses against evolving cyber threats.

The integration of artificial intelligence, AI, has emerged as a sharp, double-edged sword in the security landscape. It acts as both a crucial tool in the defense against cyber threats and as a potential enemy -- and a potent enemy, excuse me.

AI technologies, such as machine learning algorithms, play a pivotal role in augmenting cybersecurity capabilities. AI enables rapid analysis of vast datasets to identify potential threats, enhance detection, and automate response mechanisms.

AI-driven threat intelligence allows for proactive identification and mitigation of emerging risks.

Artificial intelligence has also been weaponized to extend offensive capabilities as threat actors increasingly leverage the technology to conduct more sophisticated and

targeted attacks.

Adversarial machine learning, where attackers manipulate AI algorithms, presents a new challenge that requires continuous innovation and defensive strategies.

At today's hearing, we will hear from experts on Border Gateway Protocol security. This postal service for the internet ensures that your information gets to its intended destination in as few steps as possible.

While internet-routing security might not be the most attractive topic for a congressional hearing, it is our job to discuss these security issues to protect the American public.

Again, I want to thank our witnesses for being with us today, and I look forward to our discussion and to your testimony.

At this time, I now yield to the ranking member of the subcommittee, the gentlelady from the Seventh District of California, for 5 minutes, for her opening statement.

[The prepared statement of Mr. Latta follows:]

******** COMMITTEE INSERT ********

Ms. Matsui. Thank you very much, Mr. Chairman.

I am delighted that for our first hearing in 2024, we will be exploring the modern cybersecurity landscape. It is timely and important part of this subcommittee's jurisdiction.

Over the last few years, major cyber events, like the Colonial Pipeline and ransomware attacks on hospitals, have opened American eyes to pervasive threat posed by unsecured cyber infrastructure.

For too long, this threat was treated as an afterthought or something only major financial institutions needed to worry about. Unfortunately, recent history has shown just how flawed this mindset can be.

That is why I am excited about hearings like this. It gives us an opportunity to remind the government, corporations, and consumers that cybersecurity must be foundational consideration in the digital world.

And even though the threats to critical infrastructure and corporations are receiving attention, I am worried about the equally nefarious risk less-resourced organizations and consumers face. I am especially concerned about the rise in attacks targeting America's K-12 schools.

The unfortunate reality is that cyber attacks targeting schools are increasing in frequency and severity. In 2016, the annual number of publicly disclosed cyber events was around 100. By 2021, the number has grown to nearly 1,400 annually.

But it is important to remember that these are only the attacks that get publicly disclosed. Evidence suggests that 10 to 20 times more K-12 cyber incidents go undisclosed every year.

2021 was also the third straight year with more than 50 publicly disclosed K-12 ransomware attacks, again, a number that in reality we know is much, much higher.

These incidents have threatened students' privacy and caused harmful classrooms disruptions. Alarmingly many schools simply do not have the resources to adequately combat this sophisticated threat.

That is why I introduced a bipartisan, bicameral, Enhancing K-12 Cybersecurity Act. My bill includes three specific provisions to promote access to information, better track cyber attacks nationally, and improve K-12 cybersecurity capabilities.

First, it would establish a cybersecurity information exchange to disseminate information, best practices, and grant appointees opportunities to improve cybersecurity.

Second, it would create a cybersecurity incident registry to track incidents of cyber attacks on elementary and secondary schools across the country.

Finally, and most importantly, it would deploy a K-12 cybersecurity technology improvement program to serve as a public-private partnership to boost K-12 cyber defenses. This bill has the support of major school groups like the National Association of Secondary School Principals and elementary school principals, as well as the Council of Chief State School Officers.

Technology and industry groups are also on board, like the Corporation for School Networking and the Information Technology Industry Council.

But there are also plenty we can do administratively to give our schools a boost in their fight against cybercriminals. Back in 2022, I wrote to the FCC urging Chairwoman Rosenworcel to consider ways to modernize its E-Rate program to ensure it keeps pace with modern advances in cybersecurity.

E-Rate currently allows for basic firewalls to defend against cyber attacks. This

capability falls short of what is needed to address the cyber threat landscape schools face today.

Thankfully this past July Chairwoman Rosenworcel announced her plan to create a pilot program to invest in cybersecurity services for K-12 schools and libraries.

I am also laser-focused on what can be done to keep American consumers safe. In July, I joined Deputy National Security Advisor Neuberger and Chairwoman Rosenworcel at the White House to announce the Cyber Trust Mark.

Like Energy Star, this new mark will serve as a signal to consumers that the devices they are buying are safe. From baby monitors to smart thermostats, this will raise the bar in the Internet of Things.

I am excited to hear from our witnesses today, and with that, I yield back the balance of my time.

[The prepared statement of Ms. Matsui follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Well, thank you very much. The gentlelady yields back, and the chair now recognizes the gentlelady from Washington, the chair of the full committee, for 5 minutes for her opening statement.

The Chair. Good morning, and thank you, Chairman Latta.

Cybercriminals are estimated to have made nearly $8 trillion in 2023, a number that is expected to rise to $10.5 trillion by next year. For Americans, who have become accustomed to using the internet as an essential part of life, that means their most personal information is constantly at risk of being exploited by bad actors.

Every day people are sharing more and more of their information online. We share our financial information when we pay our bills, health information when we schedule a doctor's appointment, and location information when we search for food or other essential items nearby.

We use the internet to stay in touch with family and friends, continue our education, and open new businesses. The amount of information we share will continue to increase as our technology becomes more advanced.

It is vital that we ensure the technology we use every day is safe and secure, which is why Energy and Commerce is continuing efforts to advance data privacy protections for Americans.

We need to make sure people are protected from the dangers of unsecure applications collecting their personal information unrestricted, especially apps like TikTok, which is beholden to the CCP.

At the same time, we also need to ensure the security of our overall broadband

networks, which are foundational to our economy. They enhance how people connect and create new opportunities for the hardworking people of this country.

As we become increasingly connected and more reliant on technology, this digital infrastructure that underpins our connection becomes a target for bad actors. From phishing scams designed to steal our personal information to ransomware attacks that extort money from people and businesses, the AI-generated threats, which are making it easier and easier for criminals to target Americans, the list of tools continues to grow, and the communications sector in particular has long been targeted.

2021 saw a 51-percent increase worldwide in the number of attacks on communications infrastructure. In the U.S. alone, there are more than 2,200 cyber attacks on communication infrastructure every day, averaging nearly one attack every 39 seconds.

The range of tools used by cybercriminals is extensive and growing, both in the United States and around the globe. Broadband networks are integral to the functioning of governments, military operations, and essential services.

Foreign actors, particularly those from countries with a track record of state-sponsored cyber activities, are increasingly exploiting vulnerabilities in our infrastructure in order to carry out espionage, cyber attacks, and other activities that compromise our national security.

That is why our efforts to remove equipment sourced from companies like Huawei and ZTE, which are China-owned and controlled by the CCP, are so important.

In 2020, Congress passed the Secure and Trusted Communications Network Act to mitigate these vulnerabilities. The bill established a fund for broadband providers to replace communications network equipment that poses a national security threat.

It is vital that Congress provides the $3 billion needed to fully fund this effort, and I will continue to work with my colleagues to find a path forward.

We cannot continue to allow China to access our networks or compromise our communications supply chains, especially with the increasing frequency and sophistication of these attacks.

Addressing ongoing cyber threats will take an all-of-the-above approach rather than a one-size-fits-all, one that leverages the expertise of our Federal agencies in their specific, unique sectors.

At the same time, we must ensure industry is able to innovate and adapt to evolving threats and that the government does not unnecessarily restrict industry with overly burdensome regulations that prevent it from responding swiftly to cyber threats.

This is the best way to build on American technological and communications leadership, strengthen our national security, and win the future.

I look forward to today's hearing and discussing how we will enhance our cybersecurity to protect the digital infrastructure that is vital for every aspect of our lives.

Thank you to our witnesses for being here.

Mr. Chairman, I yield back.

[The prepared statement of The Chair follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Well, thank you very much. The gentlelady yields back, and the chair now recognizes the gentleman from New Jersey, the ranking member of the full committee for 5 minutes, for an opening statement.

Mr. Pallone. Thank you, Mr. Chairman.

Today this subcommittee continues its vigilance in overseeing our communications networks and ensuring we are doing all we can to protect them from threats. These threats may come from rogue internet criminals using ransomware to extort money from hospitals, schools, and libraries, or they may come from foreign adversaries that see our networks and devices as entry points to disrupt our daily life or conduct espionage campaigns.

Protecting our communications networks from these threats is essential because the communication sector underpins a significant part of the American economy. From healthcare to energy to public safety, nearly every facet of American life relies on your Nation's communications network.

And, while the innovations and advancements that these networks enable are remarkable, it also makes these networks and the devices that run on them targets. This will only increase as more devices in our homes are connected.

Things like cars, TVs, refrigerators, gym equipment, and even light bulbs and home security systems, if they are connected to the internet, they are vulnerable to cyber attacks.

This reality means that even our homes are now subject to a cyber attack. It was recently reported that homes equipped with connected devices can face more than

10,000 attacks a week, and these attacks can give criminals insight into our movements and data about our families. They can even allow criminals to take over the device remotely.

So it is imperative that we understand the cybersecurity risks our networks and devices face to better protect our country and consumers from cyber attacks.

This committee has focused on cybersecurity on a bipartisan basis. In 2020, we came together to enact the bipartisan Secure and Trusted Communications Network Act, and this law gives the FCC the authority to exclude untrusted equipment from our communications networks after our national security agencies -- they were real risk.

This was a major step in ensuring our networks are secure from malicious foreign interference, but now this rip-and-replace program needs an additional $3 billion to fully rid our networks of Huawei and ZTE equipment. We must come together again to ensure this program is fully funded.

The Biden administration and the FCC have also taken actions to address cybersecurity in the communications sector. Last March, President Biden released the National Cybersecurity Strategy.

It takes several important steps, including shifting the burden of protecting cyberspace away from consumers, small businesses, and local governments, to software providers who are better positioned to reduce security risks.

President Biden then released the implementation plan for the strategy last July. It outlines more than 65 -- or I should say -- no -- 65 cybersecurity initiatives that Federal agencies are conducting and timelines for their completion, and that plan will be updated annually.

At the FCC, Chairwoman Rosenworcel has taken several critical actions to

strengthen cybersecurity and enhance supply chain protections. She recently rechartered the Communications Security, Reliability, and Interoperability Council and relaunched the Cybersecurity Forum for independent and executive branch regulators, which encourages Federal agencies to exchange information to protect critical infrastructure.

And the FCC has also proposed a voluntary cybersecurity labeling program for Internet of Things devices so that consumers can easily identify trustworthy devices and make safer purchasing decisions.

And, finally, while securing our communications networks and the devices that rely on them, it is imperative -- and I don't want to de-emphasize that, that it is imperative -- but I continue to strongly believe that we must also enact robust Federal data privacy protections to complement our cybersecurity efforts.

For instance, minimizing the amount of consumer data that our networks and devices have access to could reduce the consumer impact of cyber attacks.

Last Congress Chair Rodgers and I worked together to advance data privacy legislation with strong provisions focused on data minimization.

With cyber attacks becoming a more common occurrence, minimizing the amount of data collected on consumers is vital, and I remain committed to work on exacting strong privacy protections.

It is the only way we can limit the aggressive and abusive data collection practices of Big Tech and data brokers, ensure our children's sensitive information is protected online, and put consumers back in control of their data.

So I look forward to hearing from our witnesses about the challenges and potential solutions for securing our communications networks and devices, as well as

consumer data, and I yield back, Mr. Chairman, the balance of my time.

[The prepared statement of Mr. Pallone follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Thank you very much.

The gentleman yields back.

Member opening statements are now concluded.

The chair reminds all members that pursuant to the committee rules, members' opening statements will be made part of the record.

Again, the chair wants to thank our witnesses for being with us today to testify before the subcommittee, and each witness will have 5 minutes to provide an opening statement, which will be followed by a round of questions by members of the committee.

The witnesses before us today are Mr. Jim Richberg, head of cyber policy and global field, CISO, Fortinet, Inc.; Mr. Tobin Richardson, president CEO, Connectivity Standards Alliance; Mr. Alan Butler, executive director and president, Electronic Privacy Information Center; and Clete Johnson, senior fellow, the Center for the Strategic and International Studies.

And I also want to thank our witnesses again for being with us, and I also want to make note that you will notice that there is a timer light on the table, which will turn yellow when you have 1 minute remaining, and it will turn red when your time has expired.

So, again, thank you very much for being with us, and Mr. Richberg, you are recognized for 5 minutes for your opening statement.

STATEMENTS OF JIM RICHBERG, HEAD OF CYBER POLICY, FORTINET; TOBIN RICHARDSON, PRESIDENT AND CEO, CONNECTIVITY STANDARDS ALLIANCE; ALAN BUTLER, EXECUTIVE DIRECTOR AND PRESIDENT, ELECTRONIC PRIVACY INFORMATION

CENTER; AND CLETE JOHNSON, SENIOR FELLOW, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES.

STATEMENT OF JIM RICHBERG

Mr. Richberg. Thank you. My name is Jim Richberg, and I have nearly 40 years of experience in cybersecurity, including leadership roles in the Federal Government, overseeing implementation of major cybersecurity programs in the Bush and Obama administrations and serving as the national intelligence manager for cyber under two Directors of National Intelligence.

After my government service, I joined Fortinet as the head of cyber policy and global field, chief information security officer.

Fortinet is a U.S. company that is one of the largest cybersecurity companies in the world. Fortinet is best known for manufacturing over half of the firewalls sold worldwide, but its portfolio extends across nearly 60 different security and networking products.

Fortinet also operates a robust training program focused on closing the cyber workforce and skills gap and helping users become more digitally secure. We are proud to be part of numerous collaborative efforts with the Federal Government, ranging from NIST's National Cybersecurity Center of Excellence to CISA's Joint Cyber Defense Collaborative.

Our broad approach to cybersecurity reflects not only Fortinet's commitment to innovation but also a theme we believe is essential, and that is the need for partnership.

The technological environment we face today is vastly different than when I

retired from Federal service. We have seen accelerated movement to the cloud, a shift from largely wired networks to software-defined networks, a proliferation of Internet of Things devices, and a dramatic growth in the breadth and power of AI-enabled services.

Layer on to these technological changes the COVID-fueled imperative to enable remote work and offsite connectivity, and the result is that IT and communications are now laser-focused on enabling the connection of users, devices, data, and computing power regardless of where these are located and how they are provided.

Doing this securely is more than any single user, any company, or any government agency can realistically expect to meet alone. At its core, cybersecurity is a team sport.

While I go into significant detail in my written testimony, I would like to highlight for the subcommittee a few areas where effective partnership is happening now and how the U.S. Government can continue to foster collaboration.

First, any good coach tells his team, "Talk to each other out there on the field." Cybersecurity is no different. And cybercriminals talk to each other, actively partnering to bring their specific skills to a criminal enterprise.

If we are to keep up, industry and government must work together, sharing cyber threat intelligence and having interoperable cybersecurity tools and sensors.

Moreover, while companies like Fortinet and large government agencies have the resources and talent to produce their own threat analysis, this is simply not feasible for smaller organizations.

NTIA's C-SCRIP program, created by this committee for sharing risk and threat information with small telecommunications providers and equipment suppliers, is a good example of partnership to address this vital need. I urge the committee to continue to foster this kind of multidimensional and multidirectional collaboration.

Second, we need to partner in supporting consumers. It is not realistic to expect consumers to successfully go it alone in understanding cybersecurity. That is why Fortinet has dramatically expanded its award-winning free training on cyber threats and on good cybersecurity practices.

Educating users at every level is critical to our collective security. This means supporting the person using their home computer, as well as the small business owner buying a WiFi access point, and the school administrator purchasing equipment for our students.

At Fortinet, we were pleased to see the FCC take action that addresses this latter point. The Commission's recently announced pilot project will give school districts the ability to apply for funds to purchase equipment and services designed to meet 21st century threats.

And the FCC's work to create a Cyber Trust Mark comparable to the Energy Star label will help increase transparency and empower more informed purchases.

Finally, in closing, we need to work as partners who can act quickly and flexibly. And we are fortunate that to date the U.S. has taken a collaborative approach to cybersecurity with great success.

As the committee continues its good work on cybersecurity, I urge you to continue to be partners with us. Thank you for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Richberg follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Well, thank you very much for your testimony today.

And, Mr. Richardson, you are recognized for 5 minutes for your opening statement.

STATEMENT OF TOBIN RICHARDSON

Mr. Richardson. Thank you so much. Good morning, my name is Tobin Richardson, I am president and chief executive officer of the Connectivity Standards Alliance, the international standards body for the Internet of Things industry.

The Alliance is comprised of more than 700 member companies that connect consumers to the world of devices. We work together with our members to develop standards with the goal of improving the connection between people and devices to promote innovation in the most secure environment possible.

This connection is already delivering big benefits for the American people. Just to name a few, smart water pressure sensors alert consumers to water leaks, so they can be fixed before destroying a lifetime of memories.

Smart locks and sensors give families peace of mind that their home is secure. Smart thermostats help control energy costs and promote sustainability.

Historically, the Internet of Things has been characterized by custom solutions and custom hardware. If you wanted smart light bulbs, you needed the smart light bulbs, their associated gateway device, and an app to control them all.

This was not only a challenge for consumers trying to make things work together in their homes, but it also created the challenge of evaluating the relative security risk of

each piece of technology.

Some of our member companies engaged early to help consumers navigate the dizzying complexity of integrating different systems' interfaces in unique ways by creating ecosystems of devices that could work together within the moment.

Amazon's works with Alexa, Apple's HomeKit, Google Home. Samsung SmartThings are the largest and best known, but there were and are other ecosystems of devices.

This was a significant improvement over hundreds of separate options, but as an industry, we thought we could do better. That improvement is called Matter.

While still in its infancy, today our Matter standard is allowing consumers to connect smart devices from different manufacturers across the industry. Matter does this by using a common application layer, or language, and data model that delivers interoperability between devices, allowing them to communicate with each other across multiple network technologies.

As Matter was developed by our membership, integrating data privacy and security was essential to our work. That is why the Alliance developed a set of principles to guide this global standardization work.

Those principles are confidentiality and integrity, proof of identity, the use of open standards, and minimizing the data shared.

These principles aim to protect consumers and their personal information, IoT systems. As our members developed Matter, we recognized that, if we truly believe in providing an environment for data privacy, we must ensure that security is at the heart of the Matter standard.

This is why security was core to the development of Matter. Just as we started

with principles for our privacy work, the Alliance's principles on security serve as key design tenets and provide a baseline for building secure IoT devices.

First, Matter devices employ a comprehensive security approach. That means securing the device from the start, protecting every message the device sends from the moment the consumer adds it to their network, and ensuring that updates to the device are secure.

Second, security of Matter devices based on strong established cryptography out of the box.

Third, Matter devices need to be agile. As others on this panel have testified and will testify, cyber threats are constantly changing. Device security needs to be at least as adaptive as the threats it will face.

Fourth, Matter devices need to be resilient, and even though the most well-designed device will face adverse conditions, these devices need to be designed to protect themselves, detect threats, and recover from failures.

And, finally, and probably most importantly, all of this has to be easy. Consumers should not have to be part-time or full-time engineers to get the basic use of their different devices.

In addition to building consumer confidence with Matter, we support the FCC's proposed U.S. Cyber Trust Mark program. We believe this program will be most effective if it remains voluntary and focus on IoT devices.

We also recommend the FCC structure the program to allow it to be strong enough to meaningfully address IoT security, be flexible enough to incentivize private sector adoption, and be informative enough for consumers when they purchase new products.

The Alliance looks forward to working with the FCC and our colleagues in the industry, such as the Consumer Technology Association, on implementing this program.

Consumers will have a new tool that will give them confidence that the products they are purchasing are secure. They can just look for the new FCC Cyber Trust label.

Thank you again for this opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Richardson follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Thank you very much.

And, Mr. Butler, you are recognized for 5 minutes for your opening statement.

STATEMENT OF ALAN BUTLER

Mr. Butler. Thank you, Chairman Latta, Ranking Member Matsui, Chairwoman Rodgers, Ranking Member Pallone, and distinguished members of the committee for the opportunity to testify today.

My name is Alan Butler. I am the executive director of the Electronic Privacy Information Center. EPIC is an independent, nonprofit research and organizational institution here in Washington, D.C., and we were established in 1994 to secure the right to privacy for all in the digital age.

We applaud this committee's leadership in advancing strong privacy and data security standards and supporting robust enforcement to secure our communications systems and protect consumers, public safety, and our national security.

This includes Chairwoman Rodgers' and Ranking Member Pallone's American Data Privacy and Protection Act last Congress, which members of this committee overwhelmingly supported.

Advancing bipartisan privacy legislation is an essential step towards protecting privacy and strengthening cybersecurity in the digital era. By minimizing the amount of sensitive data that companies collect about us and establishing uniform data security requirements, we can reduce both the incentive and the ability of malicious actors to infiltrate our private systems.

Data breaches, cyber intrusions, and a loss of control over sensitive personal data are urgent problems that plague consumers every day, and these breaches fuel identity theft and fraud that costs consumers and taxpayers billions.

The Department of Justice estimates that, in 2021 alone, the cost of fraud to victims of identity theft was $16.4 billion, and over the last 10 years, that number has reached at least $15 billion in each report.

A report from Javelin estimates the losses from all fraud and scams in 2021 totaled $52 billion. This is an urgent problem that demands swift legislative and regulatory action.

The FCC has an important role to play, in coordination with other agencies, to ensure that we are making the best use of current authorities to combat these data abuses online.

And we encourage this committee to provide these agencies with the resources they need to safeguard and harden our communications systems against cyber attacks and misuse.

One key category of identity fraud is account takeover fraud, which costs consumers more than $10 billion a year. Our insecure communications protocols are a major vector for these account takeovers.

Unsuspecting consumers have seen their financial accounts drained, their sensitive files stolen or deleted, and have been subject to surveillance and harassment or worse.

And the vulnerabilities in our networks are also an entry point for malicious foreign actors that threaten our physical safety and national security.

The White House National Cybersecurity Strategy recognizes that harms caused by

poor cybersecurity will not be solved if we rely on market forces alone.

A secure and resilient digital ecosystem is possible only if the entities that are best positioned to reduce these risks bear some of the consequences of these breaches.

And that means first imposing limits on data collection use and transfers and establishing strong protections for sensitive data, and second, developing rules that properly align incentives for investments in robust cybersecurity protocols.

Poorly secured software and services create systemic risks, and everyday Americans should not be forced to bear the ultimate costs. The systemic cybersecurity risks that we face have been made -- has been exacerbated by the proliferation of connected devices that are insecure and create new privacy and safety hazards for users.

Consumers can often not control the level of security, nor the nature of data collected by these devices.

By implementing a labeling system like the Cyber Trust Mark, we can begin to shift incentives toward greater security while also empowering consumers with more detailed information about the types of data these devices collect.

To tackle these important problems facing Americans, EPIC encourages U.S. policymakers first to advance bipartisan privacy and data security legislation; second, to ensure that the agencies overseeing our digital ecosystem have the resources necessary to implement and enforce strong standards; third, to develop new frameworks that shape market forces toward stronger security and resilience; and, fourth, to prioritize funding and focus on improvements to core standards and protocols that are necessary to protect consumers and our communications infrastructure.

Thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Butler follows:]

******** COMMITTEE INSERT ********

Mr. Latta. And thank you, Mr. Butler, for your testimony.

And, Mr. Johnson, you are recognized for 5 minutes for your opening statement.

STATEMENT OF CLETE JOHNSON

Mr. Johnson. Thank you so much, Mr. Chairman, Ranking Member Matsui, Mr. Pallone, Members, thank you for your focus on cybersecurity. Your bipartisan approach to these issues is a welcome continuation of decades of cybersecurity policy across multiple Congresses and administrations, and this leadership has never been more urgent as our most dangerous adversaries are growing more violent and destructive in both the physical world and in cyberspace.

Russia's invasion of Ukraine and Hamas' atrocities have illuminated a nascent military alliance among China, Russia, Iran, and North Korea. Beyond physical aggression, their offensive cyber capabilities are extremely sophisticated.

So the stakes could not be higher for us and our free market democratic allies as the battlefields of today are in cyberspace as much as in the physical world.

In the 5G era of ubiquitous connectivity, the physical world will converge with cyberspace in ways we have never even imagined. This means great advances, but it also means that bad actors can attack from anywhere in the world.

The threats are clear and present, but American and allied cyber capabilities are stronger and faster than our adversaries.

And, if we do this right, this can be a success story that is uniquely American. So I urge the committee to orient its activities around the following core principles.

Number one, implement dynamic, flexible cybersecurity practices that innovate even faster than the cyber threats.

Number two, harness powerful market drivers for security, reliability, and resiliency that align directly with government interests.

And, number three, build accountable partnerships based on deep ongoing collaboration between government and industry.

The roots of this approach actually go back to the nuclear era when the Cuban missile crisis prompted the government and industry to partner together to secure telecommunications in the event of a nuclear leak.

This partnership from the early 1960s is the foundation of all present-day critical infrastructure cybersecurity activities. For example, the Communications, Information Sharing, and Analysis Center is physically co-located with the U.S. Government at CISA.

Decades before DHS even existed, network operators began working literally side by side with the government through hurricanes, wildfires, cyber attacks, routine day-to-day challenges to maintain communications through all hazards.

This is just one example of the highly capable partnership between government and the communications sector, which is so deeply engrained in our network defense that it goes unnoticed.

A good example is March 2020. We all remember COVID shifted our society to remote school and work overnight, but video conference services like Zoom were not ready for hundreds of millions of people at once.

ISPs met the unprecedented demands and worked furiously behind the scenes with the government to secure America's networks during this massive shift.

This dynamic, proactive, collaborative accountability for security prompts an

ever-improving race to the top, instead of traditional prescriptive checklist compliance, which leads to complacency at the lower common denominator.

I want to highlight four areas where the committee can advance these principles. First, as has been discussed, IoT and the Cyber Trust Mark, I think this new program is going to leverage extraordinarily powerful global market drivers throughout product development and operation.

It is based on NIST processes that are very rigorous with engineers and cyber experts. It will grant significant legal protection and security credibility to those earning the mark.

And I urge the committee to press to maximize the speed and market power of this new program by establishing the mark as an opt-in program and vigorously promote adoption, so it can move at the speed of the market.

Second, internet routing security. The stakeholders in the internet routing system are extremely diverse, complex, and even global, many well outside the FCC or U.S. Government jurisdiction.

So ISPs last year proposed a broad collaborative approach to accountability and routing security. This process is a whole-of-government and even whole-of-the-internet approach that has shown significant positive impact in its early months.

I think it is an especially effective approach to security, more dynamic and effective than prescriptive compliance, because it has engineers, not lawyers, at the table, and that is where you get the solutions. I would love to talk about that more in the questions.

Third, the Cybersecurity Framework, there has been some visionary leadership in taking proactive approaches to implementing the Framework. There are a lot of areas

that we can talk about on that, but I just want to highlight the Cybersecurity Framework is one of those American success stories.

And, finally, fourth, supply chain, we have to identify and help eliminate the untrusted suppliers from our markets. That includes funding -- fully funding rip-and-replace as it has been noted.

And then, on the positive side, we need to promote trusted suppliers. Grants from the NTIA's Wireless Innovation Fund can help do that, as can more spectrum, as we discussed back in March. A spectrum shortage means a shortage of trusted suppliers.

So, with that, I turn back my time. Apologies for going over, Mr. Chair. There is a lot to discuss, and I look forward to your questions.

[The prepared statement of Mr. Johnson follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Well, thank you very much.

And this concludes our witness opening statements. And we will now begin our members' questioning, and I will recognize myself for 5 minutes.

Removing untrusted equipment from our networks, like that produced by Huawei and ZTE, continues to be a priority for this committee. We are still working on ways to fully fund the rip-and-replace program, and it needs to be done soon.

Mr. Johnson, as we search for a solution, what is the threat posed by the continued presence of their equipment on our networks, and what other CCP threats face our networks?

Mr. Johnson. Thank you, Mr. Chair. I think that is pretty simple, that if you have untrusted equipment in a network, and that untrusted equipment has a connection with an aggressive cyber espionage and cyber attack state, in this case, the People's Republic of China, the CCP, then you have an ever-present threat in multiple ways.

The first is espionage and data exfiltration. The intelligence services can see what is on the network and whether they exfiltrate it or just surveil it, that is clearly a threat.

The second is disruption and destruction. If you run a network you can disrupt it or even shut it down. So that has obvious national security implications, but it also has a more subtle, and in some ways more dangerous, threat of coercion.

Think of how most of Western Europe gets its natural gas from Russia through those pipelines -- or at least did before the invasion. In the same way that Russia can coerce Western Europe through its supply of gas, China could coerce the United States through the operation of its telecom networks.

So I think it is a very severe threat as long as that equipment is in our networks.

Mr. Latta. Well, thank you. Thank you very much.

Mr. Richardson, last year, the FCC released a Notice of Proposed Rulemaking seeking to create a cybersecurity labeling program for IoT devices.

The U.S. Cyber Trust Mark label is being parallel to the Department of Energy's Energy Star program. Is it more difficult to create a labeling program for IoT cybersecurity than for energy efficiency, and why or why not?

Mr. Richardson. There we go. It is difficult to communicate with consumers in a way that is simple and straightforward. I think that the focus on the Energy Star program is a good one because consumers understand the value delivered by virtue of what they get by buying an Energy Star device or appliance.

So the notion of using that as a model, I think, is a smart one because it acknowledges the importance of keeping things simple.

Then your question about, is it easy to convey trust and security to consumers, is a tough one, and it is one that we think is important, and we think the Cyber Trust program is taking the right approach to that today.

Mr. Latta. Well, thank you.

Mr. Richberg, it is my understanding that the Border Gateway Protocol, BGP, is the foundation routing procedure for the internet. Is this understanding correct, and was the BGP built with security in mind?

Mr. Richberg. Thank you. No, the BGP Protocol was not built with security in mind. The good metaphor is, it is like a post office. Much as the internet itself was a descendant from the ARPANET, it was intended to facilitate robust communications, not to authenticate who was communicating or what they were communicating about.

So it is essential in allowing us to route traffic between billions of destinations, but it was not designed, in this iteration, with security as a primary consideration.

Mr. Latta. Well, thank you.

Mr. Richberg, on the topic of secure by design, what can the U.S. Government and private industry do to build systems that are secure from the ground up, and how can we, in Congress, support private industries' efforts without imposing regulations that dampen the innovation? In my last 52 seconds.

Mr. Richberg. Thank you. Secure by design and its successor, secure by default -- because when you build something securely, you shouldn't rely on people to have to figure out how to make it secure. Send it to them in that configuration -- is something that the National Strategy focused on and that I actually am part of the dialogue with government to say, how can we turn this laudatory goal into something that industry can realistically develop capability that will be impactful for consumers and that will accomplish what you want as a strategic vision.

There is a lot of ongoing dialogue about how we really make this happen. It is a work in progress, but I think it is frankly critically important because if you can get this right, coming from the IT sector, this becomes something that affects all of critical infrastructure, that strengthens security of every citizen in the country.

Mr. Latta. Well, thank you very much.

My time has expired, and I now recognize the gentlelady from California, the ranking member of the subcommittee, for 5 minutes for questions.

Ms. Matsui. Thank you very much, Mr. Chairman.

I want to go back to the K-12 cybersecurity concerns. I think most people don't think that is quite as important, but it is really very, very important. And I am especially

concerned because that is a weakness, really, in our schools' defenses to exploit sensitive data about our students and teachers.

And that is why I introduced the bipartisan, bicameral Enhancing K-12 Cybersecurity Act to boost cyber defense and protect schools.

Mr. Richberg, can you describe the severity of the threat our schools face, and do you believe my bill can better equip schools to defend themselves?

Mr. Richberg. Let me take this in reverse order. Yes, we think your bill would help with this, and on behalf of ourselves and our partners in the K-12 community and the library community, we thank you for your consistent advocacy on behalf of cybersecurity for these groups.

This is part of the soft underbelly. These are under-resourced organizations. I have had conversations with K-12 districts who say, "I would love to increase my network defenses, but that means I have to give up teachers' aides in the classroom."

It is a zero-sum game, and unfortunately they lack resources. They lack the staff to do this. These are people for whom no jurisdiction in this country is large enough to have cyber threat analysts to make sense of the kinds of threats they face and to operationalize that for their districts.

Yet, collectively, you could have an information sharing and analysis center take that kind of information, put it out, give them all collective defense on an automated fashion.

So, yes, it is critically important. Too much student data, financial data, all of this is exposed. This is a target of opportunity for criminals. There is a lot that can be done in this area.

Ms. Matsui. Okay. Well, thank you very much for that.

I want to talk more about the -- thank you very much, Mr. Johnson, regarding your explanation in the conversation you had with the chairman regarding rip-and-replace and also Open-RAN.

And I just have to say that this is a funding opportunity. We really need to do it in that way, and we all know that these programs are so very, very important.

Do you know how we could really look at this in a way that people get more engaged? I mean, we talk with our constituents all the time, and regardless of where they are, whether they are large areas or urban areas or rural areas, this is really a concern of theirs.

And many times they're waiting for the funding, particularly rural areas, when they had the rip-and-replace. And do you hear more from my type of constituents on that regard also?

Mr. Johnson. It is -- ma'am, thank you, and I just want to also commend you for your leadership securing our schools and libraries. So I thank you for that.

I think the challenge in cybersecurity and security in general is that for a lot of -- a lot of constituents and consumers, it is an abstraction. They know there is a danger, but they don't know exactly what it is.

And so maybe -- I think one way to look at this is to look at those four autocratic regimes that I mentioned upfront, especially China but also Russia, Iran, and North Korea.

Think about what they are doing in the real world and then constituents can explain that that -- can understand that that is -- that is what they aim to do in the -- in cyberspace as well. It is not an abstraction.

Those autocratic regimes want to control the way their citizens, and we, operate in cyberspace through information, through our information operations, through theft of

our information, and ultimately through control of the networks that enables our daily lives.

Ms. Matsui. Sure.

Mr. Johnson. So it is actually real, and it is real in the physical world as well.

Ms. Matsui. Okay. Thank you very much.

As cybercriminals become nimbler and more sophisticated, AI will help detect and defend against novel cyber attacks. Leveraging new cyber threat intelligence data analyzed by cyber professionals, we can isolate threats before they are deployed at scale.

Mr. Richberg, how is machine learning and AI being leveraged to identify new cyber threats?

Mr. Richberg. So we often talk about the attack surface, and what we have done -- AI is not novel. We have been using it in the industry for over a dozen years. It has the ability to allow us to characterize what normal activity is, to see what is abnormal, and as someone who ran offensive operations in the U.S. Government, you try and fail many times before you succeed.

This allows you to see them trying, figure out what they are doing, block it at point of attack, inoculate everyone globally against that threat. So this is something that has been a quiet revolution for the cybersecurity industry.

Ms. Matsui. Okay. Thank you very much, and I see my time has run out. And so I will certainly submit questions.

Mr. Latta. Thank you very much. The gentlelady's time -- pardon me -- has expired, and the chair now recognizes the gentlelady from Washington, the chair of the full committee of Energy and Commerce, for 5 minutes for questions.

The Chair. The Chinese Communist Party poses a significant threat to many

aspects of our communications sector. From Huawei to TikTok, Chinese control companies are trying to integrate themselves into Americans' lives.

We have taken steps to eliminate Huawei's threat to our networks, and now we must take action to ban TikTok, to protect Americans' national security.

Mr. Johnson, do you believe TikTok is a national security threat and should be banned in the United States? Why or why not?

Mr. Johnson. Yes, ma'am. Thank you. That is a very important question. I do think it is an extremely significant national security threat on multiple levels, and I won't take up your 5 minutes going through those, but on multiple different levels, it is a national security threat, particularly as it presently exists where we don't know and can't know what the algorithms do, what the capabilities on devices are, and what -- ultimately how the CCP might be able to use what is effectively a massive dataset of over a hundred million Americans' activities.

So, yes, extremely severe threat, I think, and I think the U.S. Government has a core interest in national security and consumer privacy to fundamentally change the way TikTok operates.

I will leave it to you all to determine whether that constitutes a categorical ban, but banning the way it exists right now and the way it operates and changing it fundamentally so that it -- the algorithm -- and the algorithms are at least -- we are at least cognizant of what it can do is, I think, a national security imperative.

The Chair. Thank you.

Mr. Richberg, in your testimony, you discuss the changes in threat and malicious activity in the digital environment. Are there specific emerging threats or attack vectors that you believe pose a cybersecurity threat to the communications industry in the near

future?

Mr. Richberg. So thank you for the question, and I look at the things that we are putting together, for instance, the growing use of space by telecommunications, capabilities like 5G in a Box, all of these are empowering, but when you put these complex systems together, I think they are introducing new vulnerabilities that we will probably find are exploitable, and that will mean that we are going to have to play catch-up on those.

So, as with any new innovation, it brings you opportunity and it brings you challenge. So I would say the fact that we are coming to things like 5G in a Box, greater portability, private networks for that, and space. Space is the emerging frontier for all of this.

The Chair. Thank you.

Mr. Richardson, what are the key challenges in ensuring the security of IoT devices? Considering the diverse range of devices and their interconnected nature, will the FCC's U.S. Cyber Trust Mark contribute to ensuring cybersecurity in IoT devices?

Mr. Richardson. Thank you very much for the question. It will go a long way, but it will take, as Mr. Richberg pointed out, a team sport -- and it will take everybody at the table understanding the complexity of the challenges that we face, but also making sure that we are doing our individual roles well.

As you do on the policy side, we will work to make sure that the global standards are done in a way that are transparent, so we all know what is going into them, are done in a way that has as many actors at table so that we have the best and brightest involved in developing those standards themselves. So it is a complex question. It is going to take all of us to do it.

The Chair. Thank you. As a followup, what steps must the FCC take to ensure the Trust Mark remains a voluntary program and does not become mandatory as regulatory agencies are prone to do?

Mr. Richardson. I think they are on the right track to making sure that industry is engaged throughout the process. In addition to that, I think some of the other areas that would be important are to reference other work done around the world.

As a global organization that we are, we work with different governments, of course hundreds of companies. That includes Singapore, it includes the European Union, as well as the U.K., and so I think as the FCC looks at this, helping ensure that there is predictability for manufacturers so that if they use the U.S. Cyber Trust Mark here in the U.S., that they can use a similar approach in other jurisdictions, and that has a lot of benefits for everybody involved.

The Chair. Would you speak to the consequences of mandating the Cyber Trust Mark?

Mr. Richardson. I am sorry, bandaiding?

The Chair. Mandating.

Mr. Richardson. Oh, mandating. The consequences of going that far and mandating, I think, are concerning perhaps at first, right, because you want to make sure that there is an opportunity for companies to want to engage on this. And it has the effect of really dragging out the process, and I think that is an important part.

The Chair. Okay. Thank you, everyone --

Mr. Richardson. Thank you.

The Chair. -- for being here. I appreciate your testimony.

I yield back, Mr. Chairman.

Mr. Latta. Thank you. The gentlelady yields back, and the chair now recognizes the gentleman from New Jersey, the ranking member of the full committee for 5 minutes for questions.

Mr. Pallone. Thank you, Mr. Chairman.

Last Congress, Chair Rodgers and I advanced the strong, bipartisan American Data Privacy and Protection Act, and this bill put consumers back in control of their data, stopped aggressive and abusive data collection by Big Tech, and required data minimization to ensure companies collect only the data they need to serve their customers. So let me start with Mr. Butler.

Do you agree that the rise in cybersecurity attacks amplifies the need for Congress to adopt comprehensive Federal data privacy legislation that implements clear rules around data minimization, and if so, why?

Mr. Butler. Thank you for the question, Ranking Member Pallone. Yes, absolutely. The rise of cyber attacks and threats to consumers is a huge reason why we need strong privacy and data protection standards in the United States.

Sensitive personal data, really the amassing of sensitive personal data, puts a huge target for malicious actors to infiltrate systems and to seize our information and to leverage that towards identity theft.

And, when companies are required to minimize the data that they collect and to delete the data they don't understand need, everyone is more secure. I also think the process of understanding what data companies collect and really mapping out where that data is helps enhance their cybersecurity posture as well.

Mr. Pallone. Thanks.

And I mentioned earlier, under the Secure and Trusted Communications

Network Act, the FCC relies on national security agencies to determine that equipment or services pose a national security threat. So let me go to Mr. Johnson.

Given the need for diligence in updating the list of equipment and services that are deemed to be a threat to our Nation, do you agree that national security agencies should work consistently with the FCC to keep the list up to date to reflect current threats?

And maybe then I will ask Mr. Richberg the same question, but we will start with Mr. Johnson.

Mr. Johnson. Yes, sir, Congressman, I think that is absolutely important. We need to -- we need to essentially stay ahead of the threat. Huawei and ZTE are sort of the easy ones. And, as evidenced by what we are still dealing with, with rip-and-replace, it is important that the national security agencies engage up front, and to the extent that it is possible, transparently, in a clear process that industry can predict and adapt to so that we are not in a rip-and-replace situation anymore.

But we need to stay ahead of the threat, identify, and remove these untrusted vendors from the market in a way that the market can navigate.

Mr. Pallone. Thank you.

Do you want to add anything, Mr. Richberg?

Mr. Richberg. Yes, sir. And, as someone who was part of many of the binding operational directives in government from a national security perspective, this is something that the national security folks look at on an ongoing basis. This was not one-and-done. This is something that should be ongoing, and we appreciate the fact that the government now has a process, thanks to the work of this committee, to do this.

You focused on the macro level, the carrier level. The reality is we are talking

about secure by design, secure by default. The U.S. and 15 allied nations, big parts of industry, are all moving in the same direction, and yet the same places where this other technology is emanating are in the consumer marketplace.

You are securing the carrier. Do you want everyone's homes to potentially have routers and devices that are not developed with security and potentially have the kind of vulnerabilities that Mr. Johnson alluded to in there?

I would suggest that you might want to extend this determination, this input from the national security community to other parts of the infrastructure so that we don't find ourselves in a rip-and-replace situation involving millions of people's homes.

RPTR ZAMORA

EDTR HOFSTAD

[11:02 a.m.]

Mr. Pallone. Well, thank you.

Now, all of you mentioned in your testimony the development of the Cyber Trust Mark that is being led by the FCC. And while I think we should do what we can to encourage companies to invest in security from the outside, it is also important that consumers have all the info and tools they need to protect themselves. And the Trust Mark seems to be one way of helping consumers, who are increasingly purchasing connected devices.

So let me go back to Mr. Butler.

What kind of information is important for consumers to understand in this context? And how should the FCC consider the amount and the format that information is presented to consumers?

Mr. Butler. Thank you for the question, Ranking Member Pallone.

I think as several members and other folks testifying here have mentioned, it is a lot of information for consumers to digest. We have recommended that when adopting a labeling system that we implement a system that has multiple layers so that -- you know, in the mark itself, in the sort of physical labeling of items, there is only a certain amount of information that can be conveyed there, but that there can be, you know, web resources or secondary levels of information that provide more detail, in particular about what data the device's collector has access to and what sensors.

I think consumers really need to know what these devices are doing and what types of, you know, data or potential threats devices might pose to them or their families.

And I think that is a significant piece of what consumers expect out of their devices, that their devices are doing what they want and not something else.

Mr. Pallone. Thank you.

Thank you, Mr. Chairman.

Mr. Latta. The gentleman's time has expired.

And the chair now recognizes the gentleman from Florida's 12th District for 5 minutes for questions.

Mr. Bilirakis. Thank you, Mr. Chairman. I appreciate it.

And I thank the panel.

Mr. Butler, I have a two-part question for you. You call on the communications systems to be improved and subsequently more resilient on cyber attacks. First, do you agree that data minimization is not enough to adequately protect Americans' personal information?

And, secondly, we obviously want to ensure America remains a leader in innovation, especially for how to make systems more resilient. Do you think there are good examples of companies using information they have collected to improve their data security systems?

Mr. Butler. Thank you for the question, Representative Bilirakis.

Yes, I agree that data minimization is an important step; it is definitely not the only step. Strong data security both requirements and, as others have discussed, the evolving evaluation and response to the threats as they evolve are essential as well. And some of that, as you point out, requires an analysis of data, what is happening in the marketplace.

I think that, you know, as an example, the data minimization provisions in the

ADPPA, as I was discussing, you know, do account for the need to process data for security purposes and research purposes to that end. And I think that there are certainly, as others have mentioned, situations where, you know, machine learning, other evaluation techniques are used to look at the nature of the threats coming in and determine the appropriate response.

Mr. Bilirakis. Thank you.

Over the holidays, a nightmarish situation unfolded for one of my staffers, and I want you to hear, because this is very relevant.

For hours, my staffer's Internet of Things-connected doorbell rang at random intervals, over and over and over again, without someone physically pushing the button. Okay? Late in the night, he then received a text message from an unknown number stating, and I quote, "Do you want me to stop calling you?"

Now, this is a great staffer, a wonderful person, who happens to be young. And he has a wife and two young children. So you could imagine the scenario.

Evidently, his doorbell was hacked into. The number was blocked. And while the motive remains unclear, my staffer immediately disabled the doorbell, reset numerous passwords, talked to two police departments, and ultimately filed a police report on the incident.

So, Mr. Richardson, is this type of event something that could be prevented, or at least incident numbers reduced, based on the Matter principles you described in your testimony and the Cyber Trust Mark program you advocate?

Mr. Richardson. Thank you so much for the question.

And I think your staff member's experience is not unique, unfortunately. Everybody at this table, I am sure, has been the victim of some form of cyber crime, and it

is touching everything that is digital.

The work of the Matter standard seeks to unify and bring in engineers and security experts from around the world to definitely bring those incidents down.

The Cyber Trust Mark, through its practices and encouraging and really getting companies to adhere to principles of better security for their devices, from not sending devices with preset passwords, to taking on business practices within their own companies to ensure that those devices are secure and resilient, will reduce those incidents, I am confident.

Mr. Bilirakis. All right. Thank you.

For the last two decades or more, we have encouraged businesses and individuals alike to take cybersecurity training that warns of the dangers of different types of scams and how to identify them. All House staff, including Members of Congress, have to take this type of training on a regular basis.

While the scams are getting more complicated every year, it seems that the ways to identify scams have remained relatively stagnant.

So, Mr. Richberg, do you think that typical cybersecurity training that is encouraged by business and government alike is outdated and provides diminished returns? And if so, how do we ensure that warnings to customers keep pace with illegal tactics by bad actors?

Again, for Mr. Richberg.

Mr. Richberg. So I believe that, as AI in particular makes spear phishing, makes those kind of attacks harder to detect, the value of user training will diminish, but that doesn't obviate it. You need to continue to do that.

And that is where Zero Trust and resilience mean we have to -- we recognize you

will not have perfection in defending your device, but we can find ways of minimizing the consequences of a successful attack.

Mr. Bilirakis. All right. Thank you very much.

And thanks for holding the hearing, Mr. Chairman. I appreciate it. I yield back.

Mr. Latta. Thank you very much.

The gentleman's time has expired.

And the chair now recognizes the gentlelady from New York's Ninth District for 5 minutes for questions.

Ms. Clarke. Thank you very much, Mr. Chairman and Ranking Member Matsui, for holding this hearing.

And thank you to our esteemed panel of witnesses for joining us today. Good morning.

Our communications sector is a critical facet of our economy, and the 21st century has seen the industry grow and evolve into a complex, interconnected web of systems fueling a range of related industries.

As such, our Nation's communication networks are under a constant state of threat from malignant actors in the cyber space. And, as policymakers, we must stand ready to fend off attacks and protect the American people.

Building off the success of the legislation I was able to pass last Congress to streamline the reporting of certain cyber incidents, the Biden administration released its ambitious National Cybersecurity Strategy in March of 2023.

I believe this national cyber plan can offer well-suited support for harmonized regulation of critical industries, including the communications industry. And I applaud the administration's commitment to defending critical infrastructure, disrupting and

dismantling threat actors, fostering security and resilience, and investing in a more safe and secure future.

Due to a number of high-profile cyber attacks over the last few years, much of my work around cyber has been focused on supporting State and local governments' cyber capabilities and defending critical infrastructure and streamlining reporting requirements. So I am appreciative of the opportunity to view cyber issues through a communications-specific lens here today.

The growing prevalence of the Internet of Things, or IoT, devices has powered the transition towards smart homes and smart cities but also significantly expands the attack surface for hackers looking to gain access to networks. And with the increase of potential vulnerabilities for hackers to exploit, it is more important than ever for private companies and government entities to share threat information with relevant parties as soon as possible.

Mr. Johnson, in your testimony, you urged lawmakers to implement dynamic cyber practices that can adapt at pace with cyber threats. Can you speak to how the reporting of cyber incidents and regulatory harmonization can help us keep up with the range of cyber threats we face today?

Mr. Johnson. Absolutely. Thank you, ma'am. And I think you are referring to the so-called CIRCIA Act, the Cyber Incident Reporting for Critical Infrastructure Act -- great acronym. CISA will be putting out those rules in March, I think is the statutory deadline.

The goal and my own hope is that streamlining and advancing reporting will create a positive feedback loop of information awareness and then response. So that is a tall order. It is a very, very significant, foundational development in our legal and

operational approach to cybersecurity.

My hope is that we can further advance this whole-of-government approach, where information that is coming into CISA goes appropriately to other sectors, other agencies, and, collectively, we create a positive feedback loop of incident awareness and incident response and best practices.

So that is the hope. It is going to take a while. But that is a pretty foundational statute.

Ms. Clarke. Well, thank you.

And since the launch of a number of new generative AI tools over the last year, artificial intelligence has become one of the most discussed issues on the Hill. And while much of the conversation on AI these days is focused on specific harms and benefits to customers, cybersecurity is too often minimized in these conversations.

That being said, Mr. Richberg, I would like to give you an opportunity to expound a bit on your opening statement. What do you see as the most relevant cyber threats presented by AI? And, conversely, how can cybersecurity professionals leverage AI tools to fend off cyber attacks?

Mr. Richberg. So, when I look at the power of generative AI for attackers, it lowers the barrier to entry. You don't need to be a programmer anymore. You can generate executable codes by launching a query. And it makes, for instance, spear phishing something easier to do. So it helps the attacker.

But, conversely, the people in security operations centers are overwhelmed by data. There is not enough of them. This becomes a tool that they can use. You can literally take an instance, drop it in, and say, "Categorize this. Tell me what to do about it for my organization."

So I look at AI and ML and say, what makes them work? Data. More specifically, big data. As in the general proposition: Who is more likely to have information about a network -- the people who set it up and are defending it, or someone breaking into it as a black box? The net advantage for AI and ML is with the cyber defender.

Ms. Clarke. Very well.

Thank you very much, Mr. Chairman. I yield back.

Mr. Latta. Thank you very much.

The gentlelady's time has expired.

And the chair now recognizes the gentleman from Michigan's Fifth District.

I hate to say that the Wolverines won, but you are --

Mr. Walberg. Go, Blue.

Mr. Latta. -- recognized for 5 minutes.

Mr. Walberg. Go, Blue. Champions.

Mr. Latta. Yeah.

Mr. Walberg. Thank you, Mr. Chairman.

And thanks to the panel for being here.

Mr. Richberg, you referenced the FCC's pilot program focused on supporting cybersecurity for schools in your written testimony.

My district has experienced multiple cyber attacks in schools, including a ransomware attack that closed schools for multiple days in Hillsdale and Jackson Counties. The attacks impacted multiple operating systems, including those that control the phones, the heating, the technology used in the classrooms, et cetera. The result was a compromise of data disrupting the learning process and severe inconvenience for

working families as well. So it touches all bases.

Can you explain why schools are particularly vulnerable as targets and how they can better protect their systems?

Mr. Richberg. So schools are very open environments. They have in some cases millions, for some of the very largest, of devices on their networks. They lack adequate cybersecurity staff.

Many of the jurisdictions in our country don't have a full-time cybersecurity professional defending them. You can outsource this service, but you get economies of scale by saying: We can regionalize this and have someone -- because many of you have the same kind of equipment in your facility, we can do that.

A lot of this comes in, really, as a service externally. It should not be incumbent on organizations to have to put cyber threat intelligence in their devices. The manufacturers are pushing this out.

So the government can help by making these funds available. Let them buy products that are state-of-the-art and able to take advantage of things that are being seen in the threat environment to defend the jurisdiction without the scarce resources having to take time from dealing with students.

Mr. Walberg. Yeah. Yeah. And, of course, schools have used so much more as a result of COVID, et cetera, so challenges there. And then you have students, who don't care, necessarily, about the attacks that can go on by what they do as well.

Mr. Johnson, there have been recent reports that the Chinese spy balloon that crossed over the U.S. used American ISP to communicate back and forth to China. This is very concerning, of course, to all of us. As telecommunications providers across the country remove Chinese technology from their systems, the CCP is still using our own

networks for espionage.

How can we address this and stop this from taking place?

Mr. Johnson. It is a great question, Congressman.

And I think I will answer first by saying, that incident was a stark example of, number one, how aggressive China's espionage activities are and, number two, how clumsy they are. They didn't mean for that balloon to go all the way across our country for that period.

And to take the flip side of what we can learn from that, I think the most important thing is -- I obviously am not privy to those -- I have seen those reports. I am not privy to what that means, about communicating with a U.S. ISP. But I do know, from my previous service in government working on intelligence issues, there is certainly a lot to learn from that and what the balloon was doing, what the ISP may know about it.

I think what we need to do to prevent that in the future is do a deep-dive after-action review of what happened, what we learned from it, and how that will change China's both aggression and clumsiness in the future.

So I think it is all about this collaboration that I mentioned in my statement, the private sector and government being on the same team to prevent this type of activity.

Mr. Walberg. And admit the truth and live the truth, yeah, in the process of dealing with it. Thank you.

Mr. Richardson, securing connected devices is essential to keeping our commercial and consumer markets safe. The voluntary labeling that we have been talking about of devices that meet higher security standards is a great way to keep consumers informed and safe.

How can government leverage existing industry-led IoT cybersecurity certification

programs to accelerate the adoption of the national IoT Trust Mark?

Mr. Richardson. Thank you very much for the question.

I think, you know, government's role is partly what you are doing today, keeping the conversation open. There needs to be an active dialogue that continues past just the creation of the mark to understand how that mark should and can evolve.

The other side of that is ensuring that you are working with other governments on those programs themselves. The greatest security is going to be in getting the most people adhering to the highest common denominator in terms of security. You can do that by working with policy professionals across the world on this. That will give companies and manufacturers an ability to, again, have that predictability of what is coming in terms of security, and it also allows you to tap into a vast resource of security experts.

Mr. Walberg. Thank you.

My time has expired. I yield back.

Mr. Latta. Thank you very much.

The gentleman's time has expired and he yields back.

The chair now recognizes the gentleman from Texas's 33rd District for 5 minutes for questions.

Mr. Veasey. Mr. Chairman, thank you very much.

And what a great hearing to talk about cybersecurity defenses. I think that we cannot have enough conversations about it. I think that we need to continue to do everything we can to raise awareness amongst the American public and even empower individual Americans to do what they can in their own small businesses and homes and what have you to protect themselves.

And, last Congress, I introduced the Cybersecurity Clinics Grant Program Act. And the bill would create a grant program at the Department of Homeland Security to fund higher-education-based cybersecurity clinics at community colleges and minority-based institutions.

Cybersecurity clinics are interactive; they are personalized workshops that provide education on the importance of protecting devices, data, and identity from physical and digital compromise.

And it is my belief that this model can really empower students. And we can start working with people while they are young, before they start their businesses and have to worry about their own households being compromised, on how they can protect themselves.

And the benefits of these clinics at higher-education institutions, I think, are twofold. The first one is that these clinics really do offer a potential path to help increase the number of cybersecurity professionals. And the clinics help underrepresented civil society organizations and State and local government agencies and small- and medium-size businesses develop their cyber workforce security.

Because, again, I think that everyone is going to have to participate sooner or later in order to get this right. And efforts like these should help set the framework for a robust and strategic pipeline that can close the cyber workforce and skills gap, also while strengthening our national security defenses domestically and globally.

And I wanted to ask Mr. Richberg: In your testimony, you discuss the need for building a resilient cyber workforce, and can you please share some of the best practices and challenges that are unique to closing the cyber workforce gap?

Mr. Richberg. Thank you very much.

We had been making progress on closing the cyber skills gap. Unfortunately, the gap is widening again. The latest numbers I have seen are 3.4 million unfilled jobs globally on cybersecurity.

Ninety percent of those jobs, companies would like someone to arrive who actually has the technical knowledge to come in and be productive from day one. So something like that approach for the community college is, in fact, a very effective way of saying, "I am giving someone hands-on experience. I am providing a concrete security advantage in the community."

Mr. Veasey. Yeah. Wow.

As all of you may know, the FCC is considering a proposal for a 3-year pilot program to provide about $200 million to support cybersecurity and firewall services for certain schools and libraries.

On the other side, we have seen the private sector backing the rise of university-based cyber clinics, including two in the State of Texas.

Mr. Richberg, what steps can Congress take to help facilitate public-private partnerships to get these clinics up and running in all 50 States?

Mr. Richberg. So this is an opportunity to say, when companies have got technology, let's make sure that students get hands-on experience with this.

Because -- and this ties into -- I know you have a lot of veterans in Texas. This is another constituency where -- my experience is, what differentiates an organization that has a "meh," average level of response from one that is actually good is -- it is not just technical talent. In their security operations center, do they have teamwork? Do people actually know how to come together to get the job done on a mission? Veterans are a good source for that.

So I think we can do a better job collectively at taking these groups who have skills, these groups who need jobs, and putting them in positions to get hands-on training and practice, and then put them in companies where they can make a difference.

Mr. Veasey. Yeah. Yeah. Well, thank you.

I know that the FCC has talked about the similarities between a Cyber Trust Mark program and the Federal ENERGY STAR labeling program. And I know that we are always trying to reach constituents, too, that speak language other than English at their home so we can also protect that particular population from being compromised.

And I wanted to ask Mr. Butler: What are the benefits of building on the FCC's multilingual approach to educate consumers about privacy and data security?

Mr. Butler. Thank you for the question, Representative Veasey.

I think that, you know, with all these programs, we have to meet people where they are and speak, literally, their language. And I think that is a really critical approach, because, ultimately, these systems are only as good as the information that they can convey to the consumers that need to know, again, whether their devices are secure, what types of data the devices are collecting. I think that is an important initiative.

Mr. Veasey. Thank you.

Thank you, Mr. Chairman.

Mr. Latta. Thank you.

The gentleman's time has expired.

And the chair now recognizes the gentleman from Georgia, the vice chair of the subcommittee, for 5 minutes for questions.

Mr. Carter. Thank you, Mr. Chairman.

I am over here, guys, in timeout.

Thank you all for being here.

And thank you, Mr. Chairman, for this hearing.

Cyber attacks, as we all know, can happen in an instant, in the blink of an eye. And they can happen to anyone, even our own Securities and Exchange Commission.

And as we have heard here today, our adversaries are getting better and better at this, so we have to get better and better at how to combat it.

Mr. Johnson, it is good to see you again. Go, Dogs. I don't know about all this --

Mr. Johnson. Go, Dogs.

Mr. Carter. -- Blue stuff, but, anyway, go, Dogs.

Mr. Johnson, help me out here. You know, everything is made in China now, so -- including a lot of the wireless networking equipment. But China has got a national intelligence law. Very quickly, briefly, what is that?

Mr. Johnson. It effectively requires any China-based company to comply with whatever -- to provide information or comply in various ways with whatever the Chinese Communist Party Government wants.

Mr. Carter. So we are buying all this Chinese wireless equipment and everything, and they have this law in effect. Should we be concerned?

Mr. Johnson. I think we should be and are, thankfully.

As I was discussing with Mr. Pallone earlier, updating, for one, the covered list to go beyond the low-hanging fruit of Huawei and ZTE and to other companies that are on the list; to have a discerning approach to where in the market we know or suspect there are particularized threats, where they could be -- as you noted, anything that is connected could be a threat, regardless of where it is made -- but where do we think

there is a particularized threat that we can address, and then we need to orient our policy around that.

Mr. Carter. Well, if you have a national intelligence law, I would suspect that that is an indication that we ought to be concerned.

Mr. Richardson, do you want to comment on this at all?

Mr. Richardson. Perhaps not on the law; I am not familiar with it. But in terms of the security of devices themselves, I think we have talked about some of the principles involved in bringing devices into networks: that you need to make sure that they are done in a way that minimizes the amount of data that is shared between devices; that they are secure; they have an ability to be upgraded over the year. So you are taking all the steps to ensure that every device that shows up in a consumer's home is --

Mr. Carter. I think that is a key point you just made: the ability to be upgraded as time goes on. That needs to be done. And that is one thing that we in Congress don't have the fortitude to do, and that is to update our laws as we should. But we need to make sure it is with this equipment, especially.

Mr. Richardson. Fair enough.

Mr. Carter. Mr. Johnson, going back to you, other countries are increasingly dependent on communication equipment manufactured by our adversaries. We know China is going to these countries and offering it to them and trying to get it in there. But they may not be as aware or as concerned about the potential repercussions.

What kind of leverage does this give those adversarial countries? And what can we do in the U.S. to provide alternative equipment?

Mr. Johnson. I think you are right, Congressman; it is not a coincidence that China has a strategic mission to spread its technology across the world. Certainly, they

want the commercial and financial benefits of that, but they also want the strategic, coercive capabilities as well.

What do we do about it? I think this is where -- and it is something I always try to emphasize. It started with me when I was a lieutenant in the Army. The United States and its allies are the most powerful --

Mr. Carter. "And its allies," that is the key. "The United States and its" -- so often we think --

Mr. Johnson. That is right.

Mr. Carter. -- we have to do it by ourselves, but we need to help our allies as well.

Mr. Johnson. We are by far the -- particularly in these issues, we are the most powerful country in history, but we are immeasurably more powerful because we have allies. And, I mean, I have seen that in NATO operations.

And you think about the powerful allies we have throughout the world. Collectively, our partners and allies and the United States make up the vast majority of the global market.

Mr. Carter. Right.

Mr. Johnson. So, if we can continually look at things through a U.S. and allies perspective, we will go a long way to securing the entire world.

Mr. Carter. Okay.

Mr. Richberg, real quickly, let me ask you this. AI, artificial intelligence, we know that it can be used by hackers to conduct attacks, but it also can be used to combat attacks as well.

What are the ways that Fortinet and other cybersecurity companies are utilizing AI

to prevent and to remediate cyber attacks?

Mr. Richberg. So we are using it to detect malicious activity in real-time. We can learn, because of the telemetry, not the contents but information about what is happening that is anomalous to customers' networks -- you know what is normal; you know what is abnormal -- and then you can put signatures in place to block that.

And we can also use this generative AI to help the understaffed organizations that actually are running security operations.

Mr. Carter. There is a lot of chatter about AI up here at the Capitol these days, as there should be. But we need to keep in mind, we don't need to fear it; we can also utilize it. So thank you very much.

Thank all of you all for being here.

Mr. Latta. Thank you very much.

The gentleman's time has expired.

And the chair now recognizes the gentleman from Florida's Ninth District for 5 minutes for questions.

Mr. Soto. Thank you, Chairman.

When we are talking about cell phones or internet, telecommunications is fundamental. Telemedicine, online education, business transactions, the cloud -- all flow through our telecommunications system. So the evidence is clear: Telecom is critical infrastructure. When I think about every major threat analysis for our homeland, from major disasters to apocalyptic movies, one common element is that our communications are disrupted and we are left vulnerable.

It doesn't have to be that extreme. We see cyber attacks daily on businesses. And we saw over 70 million Americans' data was breached through major telecom

companies just over this last year or so.

Thankfully, the Biden administration has put together their executive order, which includes defending critical infrastructure, disrupting and dismantling threat actors, shaping market forces to drive security and resilience, invest in resilient future, and forging international partnerships to pursue a shared goal.

And we in Congress have to do our part as well. Ranking Member Pallone passed the Secure and Trusted Communications Network Act of 2019. And we still need to pass internet privacy here in our committee and continue to strengthen incentives and requirements for both government and industry to have sufficient cybersecurity infrastructure.

Mr. Richberg, what keeps you up at night? When we are talking about cybersecurity breaches, what is the nightmare scenario that keeps you up at night right now?

Mr. Richberg. Well, you mentioned telecommunications, sir, which is one of the lifeline sectors, one of the SICIs, systemically important critical infrastructures. The one I put at the top of the heap is power. Because when you lose energy, as soon as the batteries run out, the other 15 in every American's lives are profoundly and negatively impacted.

We have half a dozen big, sophisticated energy companies that are world-class in their cybersecurity capabilities. Unfortunately, you also have thousands of small, rural electric cooperatives on the same grid, many of whom don't even have full-time IT staff, much less cybersecurity.

So the vulnerabilities and weaknesses in our energy sector -- power generation and transmission -- that is the security risk that keeps me awake.

Mr. Soto. And we saw those threats with Colonial Pipeline and also a near-threat in New Jersey, I believe, a few years ago with their grid. So that remains a -- thank you for helping flag that for us.

Mr. Johnson, I want to talk a little bit about Rip and Replace and also about the CHIPS Act.

You know, we tried to get telecom equipment into the CHIPS Act; that was in the House version. The Senate -- ugh, the Senate -- they took that out.

So it would be great to hear -- first, Rip and Replace hasn't been fully funded, so how critical is that program? And should this committee be looking at a next-generation CHIPS Act-like bill to incentivize domestic telecom equipment?

Mr. Johnson. Thank you, Congressman.

Yes, as I said earlier, I think fully funding Rip and Replace and, essentially, taking care of that problem that we identified several years ago with your committee's leadership, it just needs to be finished.

The next step is, as you noted --

Mr. Soto. If I may interrupt just a second, can you give us an estimate or a percentage or just an understanding of how much legacy equipment from Chinese manufacturers is still in our telecommunications system?

Mr. Johnson. I think the number that I have seen -- and this is reported publicly -- is about $3 billion.

But the good news is, we now know the scope of the problem. Before the Secure Networks Act, we didn't know how far-reaching the problem is. Now we know with some particularity how much needs to be replaced and how much it costs. So I think it is just a matter of finishing that job.

Mr. Soto. And I have heard over and over about the lack of domestic telecom equipment being made --

Mr. Johnson. Yes.

Mr. Soto. -- both in the United States and among our allies. Can you give us any vision as to what we should be doing to help boost that domestic manufacturing?

Mr. Johnson. Well, I was going to say that the flip side of mitigating the risk of untrusted equipment is to maximize trusted suppliers. The CHIPS and Science Act did a lot on that.

One thing that is within this committee's jurisdiction is the Wireless Innovation Fund at NTIA. There was a big announcement yesterday on that. Hopefully there will be a number of further grants on that to really accelerate the development of open and interoperable equipment that is aimed at developing trusted suppliers based in the United States and our allies.

And so, going back to the discussion with Mr. Carter, I think that that point is also very important, that having an ecosystem of trusted suppliers with this gargantuan market of the United States and its free-market, democratic allies is a pretty significant counterweight to the sort of autocratic market that begins with China.

Mr. Soto. And this committee must foster that telecom manufacturing ecosystem.

Mr. Johnson. Right.

Mr. Soto. So thank you.

My time has expired.

Mr. Latta. Thank you.

The gentleman's time has expired.

And the chair now recognizes the gentleman from Pennsylvania's 13th District for 5 minutes for questions.

Mr. Joyce. Thank you, Chairman Latta and Ranking Member Matsui, for holding today's hearing on the important and very timely subject of cybersecurity.

And thank you to the witnesses for being here with us today.

Three weeks ago, Xfinity, which is owned by Comcast and provides broadband service to much of central Pennsylvania, including the 13th Congressional District, suffered a major data breach. More than 35 million consumers were affected by a third-party software vulnerability in which personal identifiable information was exposed. This breach includes passwords, usernames, birth dates, and even partial Social Security numbers.

While this attack was massive in scale, it was not unique. Right now, it is estimated that Americans face a cyber attack once every 39 seconds on the Nation's telecommunications infrastructure.

The long-term effects of these data breaches can be devastating -- devastating to the individuals and devastating to the community at large, from everything from credit cards that are being opened in names, to sensitive bank and medical information being exposed.

We must make protecting Americans' private information -- we must make that a priority here in Congress. And as we head into the second session of the 118th Congress, we have that opportunity. Whether from cyber attacks or from foreign entities like the Chinese Communist Party-owned TikTok, this is information which will come under attack, and it is the congressional responsibility to address this.

With regard to healthcare, as we continue to expand the use of telehealth

services, we must ensure that patients have confidence that their data and their privacy are secure in order to use these tools and technologies effectively. Already in 2024 -- actually, just 11 days into January -- more than half a million Americans have been the victim of a data breach from their healthcare provider.

For patients in my district, being able to see a specialist via a telehealth connection can be life-changing, and it is incumbent upon us in this committee to help ensure that the patient's privacy is protected during those visits.

My first question is for you, Mr. Richberg. How would you evaluate the readiness of our current cybersecurity systems, specifically those in the healthcare field, against malicious actors and threats?

Mr. Richberg. I look at the healthcare industry as an example of operational technology, as opposed to an information-technology-heavy environment. They have a lot of IT, but in IT sometimes cybersecurity can be one of your preeminent priorities. In operational technology, your priorities are safety, reliability; and security comes in a distant third. And that, unfortunately, is the reality in much of the medical industry, especially in hospitals.

I was asked what keeps me awake at night. In terms of data that is compromised, I would put healthcare at the top of that list. Because financial data I can give you, I can help you clean up your credit history, I can even give you a new Social Security number. Your medical data is irreplaceably yours. If someone commits fraud with that and your history is now commingled with someone else, you can be killed by the wrong blood type being pulled up in a hospital.

So this is something that is vulnerable; it is hard to fix. And this is, I think, something where we need best practices, we need to help them with training. And

these are the same institutions that in some places are facing closure because they simply find it hard to keep rural hospitals open.

Mr. Joyce. Mr. Richberg, can you evaluate the readiness of our current cybersecurity systems, specifically those malicious actors, both foreign and from within?

Mr. Richberg.

Mr. Richberg. I am sorry. Evaluate the readiness of them?

Mr. Joyce. Yes. The readiness of the particular programs.

Mr. Richberg. Of the hospitals, I think, again, the large ones have got staff to do this, but small ones tend to lack cybersecurity expertise, and their equipment is focused more on operational readiness and patient care and not really on cybersecurity.

Mr. Joyce. Mr. Butler, can you address for us, please, the nefarious actors who are currently attacking the cybersecurity -- the ability of our information to remain safe? Are those mostly from within or are those mostly from outside of the United States?

Mr. Butler. I think that, you know, unfortunately for American consumers, they face a broad range of threats from cybercriminals. Cyber criminal networks operate across the globe, you know, including, you know, domestically and abroad. And, unfortunately, there is a really -- what keeps me up at night is the robust capabilities that the criminals are building to develop and deploy malicious software attacks, phishing, ransomware, as a service, right, to make it into sort of a cottage industry for cybercriminals.

So I think that it is a broad range; it is not just abroad or domestic. And I think that, as I mentioned in my opening statement, the harms that American consumers suffer as a result of this are really severe and underscore the need for swift action.

Mr. Joyce. I thank all of the witnesses for being present here today.

My time has expired, and, Mr. Chairman, I yield back.

Mr. Latta. Thank you.

The gentleman's time has expired.

And the chair now recognizes the gentlelady from California's 16th District for 5 minutes for questions.

Ms. Eshoo. Thank you, Mr. Chairman, and to our ranking member for holding this very important subcommittee hearing. I think our subcommittee has a great team in Mr. Latta and Ms. Matsui leading us, so thank you for your leadership.

And to the witnesses, I think you have done an excellent job today.

I want to thank Mr. Richberg for his 33 years of service, government service -- 33 years, that is rather breathtaking -- and your service during both the George Bush administration and the Obama administration and your work with two DNIs in our government. Bravo to you.

To each witness, I think that you have done a terrific job.

I would just note parenthetically that, as we talk about, you know, all of the threats to our national security, who presents them, what we can do about it, well over a decade ago I identified both Huawei and ZTE, and it really was hell to try and convince people of what a threat they were. And I am glad that we have caught up with the identification and that -- but how broad this is in our own domestic systems we need to take care of as well.

I also want to say to Mr. Butler that the Electronic Privacy Foundation, I think, has been the gold standard on privacy issues. So thank you for the work that the foundation has done.

Many of our local water systems across the country operate without even the

most basic cybersecurity protections -- and we are learning that there are many others that are in that lane as well -- often using default passwords that are easy to hack.

Last year, the EPA issued a memo requiring States to include some basic cybersecurity requirements as part of their regular surveys of water systems. Several Republican State attorneys challenged the memo. It was struck down, leaving the EPA unable to address this serious risk to critical infrastructure.

In November, the EPA, the FBI, CISA, and others warned that many of these control facilities have since been compromised by Iranian hackers.

So, Mr. Richardson, can you please speak to the threat the U.S. faces through poorly protected or compromised critical infrastructure, like our water, such as our local water systems? And, very importantly, what do you think Congress should do about it?

Mr. Richardson. Thank you very much for the question.

The Alliance mainly focuses on consumer electronics, but I would argue that every person considers their own home critical infrastructure. As we are aware, NIST is also looking at taking, kind of, that baseline, that consumer baseline for security and applying that across industrial use cases as well.

I used to live in Georgetown, at one point, near a water reservoir with about, I think, a 6-foot fence, and that gave you an idea for the security of the water at that time. And I think we are still seeing that very short fence in front of critical infrastructure systems and due diligence in protecting those as needed.

I think there are programs that are coming. The FCC Cyber Trust Mark will go a long way for the consumer side. I understand that the White House and the FCC are looking beyond that as well.

Ms. Eshoo. Thank you.

Mr. Johnson, in your testimony, you discussed the Secure Networks Act, the Secure Equipment Act. These are two bills I worked hard on to secure our communications network. You also -- and it has been raised by several members -- Rip and Replace.

At the top of your list, what else can Congress do to ensure our networks are secure? Is there anything that hasn't been raised yet that you would like to recommend to us?

Mr. Johnson. I think it is -- and it actually goes along with the point of the Secure Networks Act and the covered list. On the risk management side, whether it is IoT and the Cyber Trust Mark or more infrastructure security, the key is collaboration, it is having the private sector and the government be on the same team in a collaborative way, where they are both benefiting each other and filling gaps that the other can't fill themselves.

Ms. Eshoo. Uh-huh.

Mr. Johnson. To me, that is the key. That is the sort of uniquely American approach that we take.

And the private-sector entities, be it a water utility or an IoT manufacturer, they are the boots on the ground, they are the front line of our defense. So we have to make sure that we are all on the same team.

So I would say: collaboration, collaboration, collaboration.

Ms. Eshoo. Thank you very much to each one of you.

One thing that I like about the Senate is that Members have 10 minutes to question. But there are many more of us, so I understand why we only have 5. Today, I wish I truly had 10.

Thank you.

Mr. Latta. Thank you very much.

The gentlelady's time has expired at 5 minutes.

And the chair now recognizes the gentleman from Texas's 14th District for 5 minutes for questions.

Mr. Weber. Thank you, Mr. Chairman.

I believe it was Mr. Richberg, in an exchange with Darren Soto from Florida, you all talked about the -- he mentioned the Colonial Pipeline system, okay?

Has there been a -- when that happens, is there a study done, a case study? Who goes in there and looks at it and says, how did this happen, can we identify the perpetrator, and can we keep this from happening again?

Your thoughts, Mr. Richberg?

Mr. Richberg. So, sir, you are actually pointing out something where we do not do a good job at having institutional memory and institutional learning. Too often, when there is a breach, if there is a report about what happens, it is internal to the organization.

We have fora like Information Sharing and Analysis Centers. If -- I mentioned in my oral remarks, this is a team sport. We are playing without having plays for the defensive team to run. If somebody gets hit out on the field, we don't know what went wrong, we don't know how to make that not happen in the future.

So that is something where we need to do a better job at partnering. We really need to do this better, sir.

Mr. Weber. You said, I think, that schools lack the appropriate staff ratio in most -- I guess we are going to lump education institutions, colleges, schools.

Does anybody study this at all, do you know? When I say "study," looks at all the things that are needed and then comes in with a recommendation.

Mr. Richberg. Well, because education is local, this is something where -- to my knowledge, no. But this is something where I look at part of it and go, we could collectivize the security.

If no single jurisdiction could justify having someone who can take this raw threat information and turn it into something actionable for school districts, collectively all of them could certainly justify having an information center to do that. And similar -- yes.

Mr. Weber. Okay.

You further said in that exchange, I think, that about half a dozen of the energy companies had a pretty good program for cybersecurity.

Is that something that -- is that proprietary information? Is that something that can be gleaned and shared with other entities, with the other energy companies, for example?

Mr. Richberg. They do a fair amount of sharing. There is an energy-sector information -- but a lot of this is resource-based. When there is proprietary information, they strip that out. But, again, they are using largely the same kinds of equipment, so my understanding is they do a good job at sharing threat and vulnerability information.

Mr. Weber. Is there a database -- and I guess this will be a question for maybe you, Mr. Johnson -- of known, quote/unquote, cyber attackers?

Mr. Johnson. It's a great question. And, as I was discussing with Ms. Clarke earlier, the new Cyber Incident Reporting for Critical Infrastructure Act -- thanks to Congress for passing that in 2022 -- is going to create that.

And the idea -- and it actually pertains to all of your questions here -- how do we

create a positive feedback loop of information awareness, situational awareness for all entities, and then response and resilience?

So I think we are sort of collectively behind on that, but we now have the laws and processes in place to catch up very quickly and do that type of discerning analysis you are talking about.

Mr. Weber. When there is a cyber attack, is there a process, for lack of a better term, of reverse engineering, you know, finding out who that is and then actually going back at them? Is that possible?

Mr. Johnson. There is a new entity at CISA called the Cyber Safety Review Board that is kind of like the National Transportation Safety Review Board that is starting to do that.

But, again, I think a lot of these new institutions and new processes are new, so I think it behooves all of us to really press to make sure that they are, A, doing a good job and, B, that all of the learnings from those incidents are going throughout the economy, not just staying in a stovepipe.

Mr. Weber. Does the learning from those incidents also constitute their study, their approaches? And can we learn from that?

Mr. Johnson. We should, and I expect that we will. And I think that is where committees like this can play a big role in making sure that happens.

Mr. Weber. As I am kind of contemplating the discussion -- and I had to step out for a while, but -- I am thinking these are the systems I have identified as being, you know, vulnerable: power system we talked about; water systems; pipeline systems; highway systems; education systems; medical systems; military-slash-government institutions.

Does that cover the waterfront?

Mr. Johnson. Well, I think you could go on with that list further. You highlighted a number -- financial networks, the communications networks. I think there are 16 critical infrastructure sectors.

But, again, in these days, when everything is connected, a lot of those critical infrastructure sectors overlap with each other or are integrated with each other, certainly mutually dependent. So this is why this team environment of cross-sector, government, private collaboration, from consumers to businesses to the government, is crucial.

Mr. Weber. Thank you for that.

And I yield back, Mr. Chairman.

Mr. Latta. Thank you.

The gentleman yields back.

And the chair now recognizes the gentlelady from Michigan's Sixth District for 5 minutes for questions.

Mrs. Dingell. Thank you, Mr. Chairman.

I am heartened by the amount of bipartisan attention and concern that we are seeing on the issue of cybersecurity, and I look forward to continuing the work with my colleagues to address security concerns and mitigate future threats in our networks.

This committee has undertaken significant bipartisan efforts to resolve compromised networks, strengthen network resiliency, and leverage the expertise of the Federal Government and industry. But we know further risks must also be addressed in our communications technology networks, from our global supply chains and our domestic critical infrastructure, to new technologies that are now mainstream in our automotive industry. This is critical and necessary for us to continue to increase

competition, spur innovation, domestic manufacturing, and ensure the integrity of our systems.

So I want to first talk about critical infrastructure.

In recent years, our adversaries have invested substantial funds in supporting their state-sponsored champions, which are state-backed companies or conglomerates. They prop them up, enabling them to offer telecom products at a significantly lower cost compared to other global manufacturers.

This strategy has resulted in a marketplace flooded with Chinese telecom products, making it difficult for U.S. telecom companies to compete. American businesses are often compelled to opt for Chinese products to remain financially viable, creating a dependency on Chinese technology that poses cybersecurity risks and, bluntly, national security risks.

Mr. Johnson, two questions: Can you talk about the cybersecurity risks of our businesses using Chinese technology in critical infrastructure? And what tools and approaches do we have to address this challenge and promote the adoption of American-made telecom equipment?

And short, because I have lots more.

Mr. Johnson. Yes, ma'am.

As I discussed earlier, there are multiple layers of threats from this untrusted equipment, and it essentially boils down to espionage and disruption and the coercion that can come from both. So, pretty severe threat.

What do we do about it? I think we identify where there are specific articulable concerns, Huawei and ZTE being maybe the easiest example, because of the capabilities that they have. All equipment has certain vulnerabilities that you have to address, but if

you know that there is an aggressive actor behind some of the equipment, then you can articulate a risk that needs to be addressed. So we need to identify those and address that throughout the market.

The second thing is on the positive side, where we use U.S. and allied innovation to essentially outpace the adversaries. And I would never bet against U.S. innovation, and I also wouldn't bet against U.S. and allied collaboration.

So I think there is a lot that we can do to promote that trusted equipment. We have a big market that is hungry for trusted equipment. And we just need to leverage that strength through public investments but also through private collaboration and aimed at free-market competition.

Mrs. Dingell. Thank you. I wish it was quite as easy as that.

But I am going to move to the automotive industry now, which -- there seems to be part of a broader strategy employed by China extending beyond the telecom sector and penetrating other industries, which I think we are very specifically seeing in EVs and autonomous vehicles.

Mr. Richberg, what can we do to ensure that the Chinese Communist Party is not successful in its efforts to flood the market with their products and encroach upon other emerging sectors, such as the autonomous vehicle sector?

Mr. Richberg. So, at this point, I think automotive sector in general, you are dealing with -- cars are basically wide area networks with wheels. So, whether it is a fully autonomous vehicle or a conventional car, automation and digitization is ubiquitous.

This is something where, again, there is increasing emphasis on, what does "secure by design" and "secure by default" mean? We have talked a bit about Cyber Trust Mark and the IoT capability. If we figure out how to do that, then you can say,

okay, this is the expectation that your products, whether they are automotive or others, will do. This is what it meant to be securely designed, and this is what the configuration should be. That, I think, is the approach to take.

Mrs. Dingell. Mr. Chairman, I am out of time with a lot more questions, so I will have more questions for the record, and I will yield back. But this is a very serious issue for both cybersecurity and national security.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Thank you very much.

The gentlelady yields back the balance of her time.

The chair now recognizes the gentleman from Georgia's 12th District for 5 minutes for questions.

Mr. Allen. Thank you, Mr. Chairman. And I appreciate you holding this important hearing.

It is good to see all of you today, and thank you for your expertise.

It is of particular importance to my district. I am from Augusta, Georgia, and it has been recognized as the growing cyber capital of America and the world.

Fort Eisenhower is in my district. It hosts the Army Cyber Command of Excellence, or CCoE, which is the Army's force modernization proponent of cyberspace/signal/electronic warfare operations. The CCoE is home to the Army's Cyber School, which trains, educates, and develops Army's cyberspace and electronic warfare workforce. It is also home to the Army's Signal School.

On a related note, the Army's Spectrum Management School is located on the base as well. Additionally, Fort Eisenhower is home to NSA Georgia, the second-largest NSA facility outside of Fort Meade in Maryland.

In summary, my district is home to thousands of cyber and intelligence soldiers and DOD civilians, conducts daily cyber and intelligence operations in support of military and U.S. Government operations around the world.

I have been there. It is amazing, what we are doing.

In fact, the combination of NSA Georgia, Army Cyber Command, and its subordinate operational units make Fort Eisenhower the largest cyber and intelligence

operations footprint in the United States Army and the second-largest joint cyber-intel operations footprint in the Nation, second only to Fort Meade.

RPTR MOLNAR

EDTR SECKMAN

[12:00 p.m.]

Mr. Allen. Every year, roughly 3,000 people leave this fort looking for work. Studies show that 70 percent of them would prefer to stay in the area, and I agree with them.

To help meet this demand, former Governor Nathan Deal in the State of Georgia, invested $100 million to create the Georgia Cyber Innovation & Training Center.

This center is located on Augusta University's campus, and its common mission is to drive collaboration between academia, government, and industry stakeholders to educate and train a superior cybersecurity workforce. It has become the nucleus for cybersecurity research and development in education.

Mr. Richberg, Fortinet has also focused on workforce elements in the cybersecurity space like we have in Georgia, the human element, as you refer to it in your testimony. So I know you recognize its importance.

Can you talk about the gaps you see in cybersecurity workforce and how efforts like those being led at Georgia's Cyber Center can help fulfill these needs.

Mr. Richberg. Thank you, sir, and we recognize we actually have created an award-winning online cyber curriculum that starts all the way at basic cyber hygiene and best practices for general users and goes all the way up through expert knowledge that would allow people like transitioning veterans to be able to leave the Service with the kind of skills that would allow them to go into a security or a network operations center and say, "Oh, yes, I know that equipment; I am fully productive on day 1."

We have not only got this broad thing, which has given over 1.3 million

certifications, we have got a separate program focused on veterans. We take that technical training and we say, "Yes, and we can help you with job placement. We can help you write your resume."

I have seen studies that show that roughly 40 percent of companies in this country that are looking for cyber talent would preferentially like to hire veterans.

Mr. Allen. Exactly.

Mr. Richberg. They recognize they are hardworking. They recognize they know mission. Help the veterans tune their resumes, tune their skills to help meet that need. 200,000 are leaving Service every year.

Some of them leave because their spouses can't find jobs, so we have made this program available to the spouses of current military employees.

Mr. Allen. And they already have the highest security clearance, so.

Mr. Johnson, how can institutions like Fort Eisenhauer and of course the innovation campus and everything we have got going on help strengthen our cyber defense? What else do we need to do?

Mr. Johnson. Thank you, Congressman. I am personally thrilled to get this question. I bought my first Army uniform there in 1992 when I was on my way to college and ROTC. I now live a few hours up the river in Rabun County, so.

And I have been back to the range. Michael Shaffer is doing some great things there. I think it is a perfect example of DOD and the Federal Government investing in a community that has a tremendous opportunity for growth, and the State.

So you get everything from the veterans that Jim was talking about, to local students who want to get into this type of work, companies that want to participate in the range, and it creates this really dynamic ecosystem of education and operation. So I

think the sky is the limit for it.

Mr. Allen. Well, when you lump in Savannah -- yeah, when you lump in Savannah River Site, we have got the largest collection of intellectual capital in this area, I think maybe anywhere in the world.

Mr. Johnson. Absolutely.

Mr. Allen. Great. Well, thank you so much.

Mr. Johnson. Yeah.

Mr. Allen. I yield back.

Mr. Latta. Thank you very much.

The gentleman's time has expired, and the chair now recognizes the gentlelady from New Hampshire's Second District for 5 minutes for questions.

Ms. Kuster. Thank you so much, Mr. Chairman, and thank you to our panel.

It is no secret cyber attacks are on the rise across the Nation, and these threats are becoming more dangerous and sophisticated every day. In my district in New Hampshire, towns, businesses, school districts, hospitals, and even police departments have been targeted by cyber attacks ranging from phishing to ransomware.

Last year, the school districts in my district, Nashua and Hinsdale, were both the target of ransomware attacks.

Congress needs to step in to protect the sensitive data of our schools and students. So I have cosponsored the Enhancing K-12 Cybersecurity Act to establish a program to address cybersecurity threats to school systems and provide resources to ensure that schools can best protect against these attacks.

I want to thank my colleague, Representative Matsui, for her leadership.

Mr. Richberg, can you speak to why school systems are increasingly becoming

targets of these attacks and what other steps Congress should be taking to prevent them?

Mr. Richberg. So these jurisdictions are under-resourced. They have lots of high value information ranging from student records to medical records to financial data, you know, and their focus really is on providing education.

So this is an opportunity to educate staff, to help educate students, to actually -- and we talked about, we have a workforce of skills gap. Some of these people are going to look at this and say, "This is interesting"; this becomes something, catch them young, even at the K-12 level.

If you get some people not only understanding the basic rules of cybersecurity, but saying, "Yes, I want to do this," this is something where we can do that, and again, we need to automate a lot of the equipment and capability because these jurisdictions do not have -- and I don't think ever will have -- the staff to take care of themselves.

Ms. Kuster. Thank you. I remain committed to working with all of you and with our colleagues to bolster the cybersecurity of our school systems.

We also know that cyber attacks expose sensitive information to our towns. In my district, a particularly heinous cyber attack defrauded a very small town called Peterborough, New Hampshire, out of $2.3 million in taxpayer dollars, which was a real blow to this small, rural community.

It is actually the town that is the model for the play "Our Town," so it is a wonderful, beautiful place, and it was tragic.

Can you speak to why small towns and rural communities may be especially vulnerable as well?

Mr. Richberg. They share the same characteristics that the school districts do. I am hard-pressed to find a small jurisdiction that even has a full-time IT person. It is

often outsourced, hopefully within your State or somewhere in the U.S., but I wouldn't bet the farm on that.

And they seldom will have someone doing cybersecurity even as a part-time job, and yet, as you said, they are dealing with sensitive data, providing essential services in their community. They share the same vulnerabilities, the same lack of resources.

Your jurisdiction paid $2.3 million. Was it the jurisdiction, or was it its insurer? Insurance has become something where it has been good and bad. It is good that if in order to get insurance, you have to say we are doing the following things.

But, because the fact that you have purchased insurance is probably a matter of public record, we have seen ransomware groups preferentially target these vulnerable jurisdictions for the easy pay-out, saying, yes, this is a jurisdiction of 10,000 people, but they have insurance coverage up to this amount.

Ms. Kuster. Great. Thank you.

Another important tool in the fight is the new Cyber Trust Mark program being led by the FCC. Much like the Energy Star labels for energy-efficient devices, the Cyber Trust Mark program will label smart devices to meet the best cybersecurity standards.

Mr. Johnson, as the FCC considers the best path forward for the Cyber Trust Mark, what steps can the agency take to drive national adoption and ensure the program has flexibility to respond to evolving threats?

Mr. Johnson. Thank you, ma'am. I think this is a very promising program. I think, as I was discussing with Mr. Richardson earlier, I think it is going to fundamentally change the market on IoT -- IoT security because it will make clear similarly to the way that Energy Star has for consumers on energy, but even more importantly, more broadly through the market, not just the U.S. market but the global market. It will matter to

retailers.

And so it is one of these things that will, if we do it right -- and I think the FCC and the broader U.S. Government is on the path to doing that -- earning this mark will create legal protections that don't exist for those who don't -- who don't earn the mark.

And so the biggest thing we can do is push it and do a massive awareness campaign to consumers certainly but also to the big box retailers that will be selling these products, to make sure that --

Ms. Kuster. I hate to cut you off.

Mr. Johnson. Yeah, absolutely.

Ms. Kuster. My time is up. I yield back. Thank you.

Mr. Johnson. Thank you.

Mr. Latta. Thank you very much. The gentlelady's time has expired, and the chair now recognizes the gentleman from Ohio's 12th District for 5 minutes for questions.

Mr. Balderson. Thank you, Mr. Chairman, and thank you all for being here today.

Americans today have IoT devices all throughout their homes -- I apologize, this first question is for Mr. Richardson, so heads up, Mr. Richardson, sorry about that -- smart speakers, vacuums, kitchen appliances, baby monitors. The list goes on.

Many of these devices use cellular modules to enable them to connect to the internet. My concern is that many of those modules are manufactured in China.

So, while we are working to rid our communications network of Chinese equipment, to rip and replace, we are allowing Chinese cellular modules to be used in IoT devices throughout the Nation.

Mr. Richardson, do you believe that the Chinese cellular modules that are used in many IoT devices pose a cybersecurity threat?

Mr. Richardson. I would -- thank you very much for the question and the interest. Our organization is a global organization. We believe that security is enhanced and improved by getting everybody at the table and getting them all to agree to fair playing practices and a level playing field. We think that security is improved that way.

When you do that, when you bring in a global organization or a global community, you also bring in a diversity of providers, and that allows a different regions and different markets to choose which ones they want to bring into their individual markets.

So we are grateful that we have hundreds of companies, module providers, from Taiwan, from Europe, and several others to put into devices around the world and let markets decide which ones are appropriate, whether that is by the consumer choice or by regulation.

Mr. Balderson. Okay. Thank you very much.

My next question is for Mr. Johnson. Mr. Johnson, good afternoon. I want to follow up with you on the use of Chinese cellular modules in IoT devices. I personally am not comfortable with the widespread use of these modules in these devices.

Do you believe that Chinese cellular modules pose a national security threat to our networks, and what does that threat look like?

Mr. Johnson. Thank you, Congressman. It is a very important question. I think it gets to the heart of some of the things that we have discussed throughout this hearing.

Number one is, can the U.S. Government and its allies identify an articulable threat emanating from a particular Chinese company, or Russian company in the case of Kaspersky Labs.

But, if it can, and as it has in the Huawei ZTE setting, then I think we have a particularized risk with that particular company.

The second look is more on the technical side. What can the device or, in this case, module do? And, if there is a link between the capability on the government side and the capability on the technical side, then that is where I think issues like the covered list come in.

And that is where we need to have clear processes for doing that type of discerning analysis.

Mr. Balderson. Okay. Let's do a followup. I understand we cannot go into every home and business in America and remove IoT devices with the Chinese cellular modules.

With that said, though, do you think it would be beneficial for Congress to act on this issue and pass a bill that would prohibit the use of Chinese-made cellular modules in IoT devices sold in the future?

Mr. Johnson. It is a great question, and I think here a scalpel is more valuable than a machete, and I think we need to take that discerning look where it is three layers.

Number one, can we articulate a threat coming from a particular company? Number two, what does the technical widget do within the, in this case, IoT? And then, number three, can any risk be mitigated or fully addressed by the things that Mr. Richardson and the Cyber Trust Mark will be doing?

It may be that there are a lot of commodity-type devices that could pose a risk but don't because there are easily implemented mitigation measures. So, in that case, that would be a much better approach.

This is why I feel so strongly about the Cyber Trust Mark. I think it is going to

clean up a lot of the sort of what you might call poor hygiene out in the -- out in the market, and it is going to let the secure devices essentially corner the market.

Mr. Balderson. Okay. Thank you very much.

Mr. Chairman, I yield back.

Mr. Latta. Thank you very much. The gentleman yields back, and the chair now recognizes the gentlelady from Texas' Seventh District for 5 minutes.

Mrs. Fletcher. Well, thanks so much, Mr. Chairman, and thank you to Ranking Member Matsui for having this hearing today, and thank you to all of our witnesses. I think this has been a really, really useful hearing, lots of great insights, and I have appreciated your perspectives on, in particular, a lot of the vulnerabilities that we face, the discussions around schools and other things that we really need to be focused on in our committee. And so I just want to thank you all for your comments today.

I do want to keep the focus a little bit on a couple of different kinds of vulnerabilities, and so I will go straight with my questions to you, Mr. Butler.

You described the vulnerabilities of SMS-based text messages to redirection attacks in your testimony, and as you noted, the attacks where a malicious actor receives messages meant for the victim, they are particularly dangerous because core security services like account validation, two-factor authentication, all the things that we are relying on now, are built on top of SMS.

So it seems like it would be difficult for consumers to be able to protect themselves from this type of attack. Are there best practices for consumers to help prevent this? Are you aware of companies taking steps to prevent these types of attacks? Can you just talk a little bit about those issues for us today?

Mr. Butler. Thank you for the question, Representative Fletcher, and I agree it is

a really important area of vulnerability to focus on, especially because, as you mentioned, SMS is used in so many circumstances as a backstop for other security measures, right? So it is really upstream of the problem.

And I think, from a consumer perspective, the best thing individuals can do, where possible, is use non-SMS-based multifactor authentication. The unfortunate thing for consumers is not all, you know, vendors and apps and services offer that as an option.

So it is really critical for the vendors, the apps and services, to, you know, expand and enhance their multifactor options so that SMS is not the only option.

In terms of, you know, further research and work being done, I think there are research in two ways to secure -- better secure SMS, given the fact that it is still a very widely used option, but it really requires action at either the network level or the platform level. And so it is, itself, upstream of even the companies that are deploying it.

Mrs. Fletcher. Okay. So that sounds like an area where we need to be particularly paying attention and focus because there is a lot of work still to do is what it sounds like. Well, thank you for that.

I know another area where we have been focused in this subcommittee and in the full committee is on artificial intelligence, and I want to touch on that briefly as well.

Last fall this subcommittee had a hearing on artificial intelligence in our communications networks, and many members, including me, focused on the potential harmful impacts of AI when unrepresentative data is used as an input.

And I want to sort of take that conversation a step further and discuss kind of the cybersecurity of common AI products like ChatGPT and the potential for malicious actors to attack those systems and manipulate the output, so not just sort of unintended consequences of the inputs but actual manipulation.

And so, Mr. Richberg, I want to direct these questions to you. Can you talk a little bit -- I have got about 2 minutes left -- can you talk a little bit about whether artificial intelligence systems are models for cybercrime and just kind of then open it up to the whole panel if we run out of time here, for you all to submit for the record kind of your response on these AI issues.

But really, Mr. Richberg, do you have kind of recommendations for minimum security measures for new AI models before they become open source, and anything else that you want to add?

We are going to run out of time, so if everyone else can just weigh in on that in writing, I would appreciate it. Thank you so much.

Mr. Richberg. Thank you, ma'am. I will move fast. I think I have already addressed that. I think the cybersecurity industry is mature in its use of cybersecurity. So let me direct this to generative AI.

My sense is, the people who are making the large-language models recognize there is concern that organizations are going to put queries in, and they are going to expose sensitive data. Roughly 1 in 10 queries does that from an enterprise perspective.

And similarly there are ways that you can do data loss prevention with a third-party program to prevent it.

The guardrails are largely being created. Where we are in the Wild West situation is, the onus is still on the consumer to ask for those. There are good protocols and protections. You simply have to stipulate what you want.

Organizations, in many cases, are moving slowly to adopt this. The risk -- you have probably heard the term "shadow IT" -- things that happen that the organization isn't aware of. Generative AI is the latest form of shadow IT.

People are saying, "I use this at home; why can't I use it at work?" They are doing it, and in many cases, they are exposing organizationally sensitive data.

Mrs. Fletcher. All right. That is really helpful, and I just went over my time, so I appreciate all of your testimony and I appreciate you holding this hearing. Thank you so much, Mr. Chairman. I yield back.

Mr. Latta. Thank you. The gentlelady's time has expired, and the chair now recognizes the gentlelady from Tennessee's First District for 5 minutes for questions.

Mrs. Harshbarger. Thank you, Mr. Chairman. Thank you, gentlemen, for being here today.

You know, we have got 15 billion devices worldwide, expected to double by 2030. We have a cyber attack every 39 seconds, and your comments have solidified why we are having this hearing today.

And, Mr. Richberg, just for the record, you have renewed my fear about healthcare vulnerabilities. And I will tell you something else I am worried about is supply chains, and honestly, really, it concerns drug supply chains, which are absolutely critical to the safety of all Americans. And that is my expertise, being a pharmacist. So I just wanted you to know that, that that is at the top of mind for me, sir, so.

Mr. Richberg. That is what we used to do in the intelligence business. Seriously.

Mrs. Harshbarger. Yeah. It is a little worrisome, yeah.

But, Mr. Richberg, as Members of Congress, we have to be tremendously careful with our information for fear -- you know, with security, for fear of nation-state actors really attempting to access sensitive information we are provided. And we are human beings, if you didn't know that, and I am telling you, we are the limiting factors. We are

the vulnerable gateway in protecting the security integrity of our connected devices. So my question to you are, what best practices should we be following?

Mr. Richberg. So I will give you the big four.

Mrs. Harshbarger. Okay.

Mr. Richberg. Enable patching. When we see -- we have talked about vulnerabilities. When we see problems, allow the vendor to -- turn your machine on so that it can update by default. That is number one.

Strong unique passwords on every device. We are human beings. We like to recycle. I may use a strong one. It is probably the same on too many systems.

Mrs. Harshbarger. Yeah.

Mr. Richberg. If it is really important data, use multifactor authentication, not just my password, something else, and please, please back up. You do those four, you do a lot to min- -- I have another set of four, but if you do those four, then we can have the second conversation.

Mrs. Harshbarger. Well, fantastic. I think I am doing four, but I will double-check.

Mr. Johnson, with China threatening to take over Taiwan, who produces the majority of our advanced chips, by the way, you know, I am listening to all four of you gentlemen today, and we could find ourselves in a scenario where we need to rip and replace consumer devices to protect our informational security. And you stated -- I assume you agree with that, sir?

Mr. Johnson. I think we need to make sure we don't get to the point where we --

Mrs. Harshbarger. Exactly.

Mr. Johnson. -- where it -- because in some cases -- it is one thing to pull out

Huawei gear from, you know, a handful of known operators throughout the United States. It is another thing to replace millions and millions of consumer devices. In some ways, probably not doable.

Mrs. Harshbarger. Yeah.

Mr. Johnson. So we have to go get ahead of the threat, both in -- as I was saying before, in identifying the particular companies and devices that are problematic, and, number two, having mitigation and the things that the Cyber Trust Mark will do.

On IoT, we need to expand that, writ large.

Mrs. Harshbarger. Well, you stated in your testimony that American and allied cybersecurity capabilities have to be stronger and faster and more capable than adversarial nations. And, in your opinion, how long are we going to be stronger and faster than our adversarial nations?

Mr. Johnson. Well, I think that is the question of the moment, and I think that question is different now than it was even a couple years ago before Russia invaded and before the atrocities by Hamas.

Mrs. Harshbarger. Yeah.

Mr. Johnson. We now have a clear picture of those four autocratic adversaries, in some cases enemies, and all of their criminal proxies that work under and around them. So we have to be as strong and agile and fast as the bad guys are.

I think we are, but it, as I said in my prepared statement, it really depends on maximizing this collaboration between private sector --

Mrs. Harshbarger. Yeah.

Mr. Johnson. -- and industry.

It also includes -- and I was talking about with Mr. Allen -- you know, the academic

institutions, the government institutions. But it is really about operational and strategic collaboration between the vendors, the service providers, and the government.

Mrs. Harshbarger. Well, I go back to being on Homeland last session, and we had SolarWinds, and we had Microsoft -- and then you look at Colonial Pipeline. It has to be an integrated effort --

Mr. Johnson. Right.

Mrs. Harshbarger. -- in my opinion.

Mr. Johnson. Right.

Mrs. Harshbarger. And, from what we are told about all these AI hearings, we are about a year ahead of China with that. So it is a little worrisome. We need to get up to speed and be ahead, be number one, which is where we want to be.

Mr. Johnson. Yeah.

Mrs. Harshbarger. Okay. Mr. Chairman, with that, I yield back.

Mr. Latta. Thank you.

The gentlelady yields back, and the chair now recognizes the gentleman from California's 29th District for 5 minutes for questions.

Mr. Cardenas. Thank you, Chairman Latta and also Ranking Member Matsui, for having this important hearing, and I would like to thank the witnesses for sharing with us your expertise and your opinions on these matters.

We have seen already how vulnerable we all are to cyber threats. For example, on December 1st, 2022, a cyber attack caused a nearly day-long outage of the 988 suicide and crisis lifeline.

People who tried to reach the line for help with suicidal and/or mental health crisis situations were greeted with a message that said the line was experiencing a service

outage.

We are talking about right in the middle of a moment where people feel compelled to get immediate help, in some cases, to prevent deaths.

Even a day's outage for a critical lifeline like 988 or 911 can have serious repercussions for those experiencing an emergency.

Mr. Richberg, can you speak to some of the vulnerabilities phone lines like 988 have to cyber attacks, and what can we do to make sure that critical lifelines like this remain secure?

Mr. Richberg. Thank you. We often talk about confidentiality and availability of services, and you are talking about one where it definitely hit the availability.

We have also seen, if someone's calling a line like that, you want it to be confidential. You don't want a risk that there may be a breach that is going to expose that I have asked for this kind of help.

And you have heard of swatting, where someone sends emergency services in place. So you need to worry about all three kinds of attacks against those.

Resilience is another thing that -- we have mentioned resilience a lot in this hearing. Resilience means having multiple paths and ways to do things. If you genuinely had an outage with the local service provider, you would like the ability to roll over to some other place, in the same jurisdiction somewhere else.

So there are -- we can talk offline about specific best practices, but I would say, worry about the confidentiality, the integrity, the availability, and ways of providing resilience for core services like that.

Mr. Cardenas. Thank you. Resilience on the cheap is something that unfortunately the average American doesn't realize when policymakers, whether it be

Congress or individual organizations make decisions, that redundancy tends to be cut out when people are trying to be, quote, more financially efficient.

But, in the long run, when you eliminate redundancy -- and what I heard, Mr. Richberg, you refer to from my vantage point is, redundancy is important, in other words, going to another secondary or another tertiary place for that service not to go down, for that accessibility to continue.

Mr. Richberg. That is an excellent point. And redundancy used to mean I have surplus capacity, more of the same.

Mr. Cardenas. Correct.

Mr. Richberg. We have now reached the point where there are multi paths to do it. I may have fiber. I may have satellite. I may even have dial-up. And it can seamlessly roll over. So it is not a matter of saying "I need three times of the bandwidth of T1 lines," but rather to say, "I have multiple ways to do it."

And the nice thing about it is, it gives you better service because if you just get degradation just due to normal traffic things, traffic can reroute and say, "This is slow; I will go the other way."

So it can actually give you a better day-to-day experience as well as that rainy day "I have an emergency" resilient system.

Mr. Cardenas. Well, in my backyard, we have L.A. Unified School District, and there was a leak of 2,000 student assessment records and some other critical information on those individuals and their families.

Mr. Richberg, I understand you are familiar with this case. Can you talk a little bit about what vulnerabilities allowed this kind of attack to be successful on them and how we can do a better job of preventing students' data, children's data, from being

accessed?

Mr. Richberg. So I think we have said that we have too few cybersecurity experts in schools. We are spending our funding, I would argue with good reason, on student-facing, educational technology and not as much on cybersecurity.

And my understanding of the L.A. Unified case is, a human discovered that while it was happening. We talk about zero trust as an operating philosophy. It doesn't mean we don't trust people. It just means we don't trust by default, and we give you the minimum amount of privilege you need to get the job done.

You would think if we were doing zero trust in the L.A. Unified School District, the policy could have said, someone should not be exfiltrating 500 gigabytes of data no matter who they are in the school district.

So there are basic principles and technologies, sir, that could be brought to bear to help L.A. Unified.

Mr. Cardenas. Okay.

Mr. Richardson, can you comment on how important it is to make sure that we have baseline requirements, like authentication for IoT devices, which would go a long way to help combat cyber threats on our networks?

Mr. Richardson. Thank you very much for that question and the point. Absolutely, authentication is a key component of Matter. It is really important that, as you look at devices coming into networks, being joined into your smart home, that they are secure, you know that they are supposed to be there, and there is a way to upgrade and update them as appropriate. So authentication is a very important part of that process.

Mr. Cardenas. Thank you.

My time having expired, thank you, Mr. Chairman. I yield back.

Mr. Latta. Thank you very much.

The gentleman's time has expired, and the chair now recognizes the gentleman from California's 23rd District for 5 minutes for questions.

Mr. Obernolte. Well, thank you, Mr. Chairman. Thank you for all of our witnesses on this really important hearing.

Mr. Butler, I would like to start with a question for you. It seems to me like the majority of the consumer cyber fraud that occurs is a result of a cybercriminal posing to be someone or an organization that they aren't.

There isn't a day that goes by that I don't have a phishing email purporting to be from my bank or from my credit card company.

It has got to the point where I don't click on any links in any email; I will go to a web browser and use a bookmark to make sure I am going where I think I am going.

And I never enter a password anymore without double-checking. If it is not on my electronic key chain and gets entered automatically for me, I ask the question, am I really where I think I am.

But, having said that, something happened the week before Christmas that just still blows me away with its sophistication. One of my employees in the private sector, not in government, got a text, supposedly from me, which was unusual, because I don't -- I am not involved with the day-to-day running of the company. But, you know, I am the boss, so he, you know, responds to this text.

The text said, "Are you doing anything? I need you to do something for me."

And he said, "Sure, what do you need?"

And the text said, "Well, is there an Apple store nearby?"

And he said, "Why, yes, there is."

And he says -- this, you know, purportedly from me -- says, "Well, I am trying to surprise the employees with some Apple gift cards. Could you go down and buy a bunch for me? And don't tell anybody. It is a surprise."

And if you think about it, I mean, the level of sophistication in that cyber attack is stunning because they knew who I was. They knew my position in the company. They knew who the employees were. They knew what my cell phone was.

And fortunately my employee thought it was suspicious that this conversation had not occurred in the same chain as the other text messages that we have exchanged over the years, and so he asked -- you know, called me and asked the question.

But, I mean, it is just incredible, and this is going to continue to happen. And I think it is -- you said something, Mr. Butler, in your testimony which I thought was really compelling. You said, it is unrealistic to expect that consumers would have the tools by themselves to distinguish what is fraudulent from what is real in this context.

But here is my question. I am really frustrated about this because it seems to me like we have the tools to fix this problem. And it is the way the big companies do it.

When you and I establish a relationship, we can exchange credentials which establishes an encrypted communications path between us, and then not only when I get something from you can I verify that it is from you, but it is also end-to-end encrypted so people in between us can't read our messages.

And don't even get me started on the fact that we are still sending emails in plain text.

So why on Earth, if we have the tools to solve this problem, and 90 percent of this cyber fraud goes away if we do that, why have we not done that?

Mr. Butler. Thank you for the question, Representative Obernolte. I think it is a really important area of focus, a really important position of vulnerability in our systems.

I mean, I think that the vulnerability of our -- SMS is still the dominant, text-based one-to-one, you know, telecommunications service, and the fact that so much rides on top of it, so much relies on it, means that vulnerabilities in that system have systemic impact.

And I think we have simply not invested the resources and time necessary to solve this problem at the systemic level. As you mentioned, the technology exists to have secure and authenticated communications, but we don't implement that adequately in the legacy protocols that people actually use.

And this has particularly significant impacts for vulnerable communities that don't especially -- you know, a variety of different vulnerable communities that don't have access to the more modern and secure systems.

So I think it really is a lack of investment of both funding, research, and the time and attention necessary to change something at such a systemic level.

Mr. Obernolte. I think there is a huge opportunity here, maybe for a public-private partnership or something that establishes for a consumer a clear and easy-to-follow path for secure communications that avoids some of these vulnerabilities.

Mr. Richardson, you talked about the security of the Internet of Things, which is a concern that I also share. One thing that you did not mention is, apart from the vulnerabilities that are involved with our communications with the IoT, the fact that there might be malicious actors who are manufacturers of IoT hardware.

And, in many of the same ways that we had concerns about Huawei and the

rip-and-replace that resulted from that, what can we do to protect against those kinds of threats?

Mr. Richardson. Yeah, no, it is a really important part -- point to that, and our approach and the way that we think about that is open -- open global standards. I talked about those principles early on for the Internet of Things.

If you are going to be bringing billions of devices into the world, you want to make sure that they are as secure as possible. You do that by bringing as many players together, especially on the commercial side, who are interacting with these devices. And that is at the core of what we do.

The second part of that is, you embrace standards that are open and transparent. All of this has to be done with sunshine and sunlight on it in order to be under the microscope of anybody that wants to examine how that particular technology is being brought into the market.

And so that transparency, that open and global approach, is the way that you really address that best.

Mr. Obernolte. Well, I see I am out of time, but let me add one thing to that, which is that I think we ought to empower the Department of Commerce to regularly update the Entity List with known malicious actors in the IoT space and use that to prohibit access to markets. I think that just makes sense.

But thank you, gentlemen, for your passion on this topic.

I yield back, Mr. Chairman.

Mr. Latta. The gentleman's time has expired, and the chair now recognizes the gentleman from Texas' 11th District for 5 minutes for questions.

Mr. Pfluger. Thank you, Mr. Chairman, and thanks for being here. I know you

guys have gone through a lot of the questions already. Let me talk about the energy sector, and I will address Mr. Richberg.

In your opinion, what makes that sector stand out today? What keeps you up at night about it? And I guess, more importantly, what can we be doing about that here with the energy sector, writ large?

Mr. Richberg. So what keeps me up at night is that it is, in my opinion, the most critical of the 16 critical infrastructure sectors. Because, when you take away power, they all fail, and everyone's life is fundamentally affected.

The challenge I see is that it is not a monolithic sector. Not only do we have oil and natural gas and electricity, but you have power generation and then power distribution.

You have players of dramatically uneven size, and they are ranging from the big energy corporations that are Fortune-sized companies with sophisticated cybersecurity, down to rural, electric cooperatives where people drive around in pickup trucks and don't even have IT support.

And yet they are all on the same grid in the case of electricity. So it is this interdependence. It is this overarching vulnerability. It is the fact that for energy, for electricity, it is a regulated industry. They don't get to say "I need to spend more money on cybersecurity" and raise their bills without a protracted process.

So there is a partnership. Government has to say they need to change -- they need more to fix this.

A lot of these smaller organizations are not cyber-aware. They are not doing the -- we have talked about they are doing default passwords. So very vulnerable sector, hypercritical, and it is something where -- unlike the financial sector where they

can say, "I need more money, no problem, I am going to raise my rates" -- they can't.

Mr. Pfluger. The nuclear plants are a closed system. When you think about that model and then look at what DHS is doing with CISA, and I guess as you kind of look at those as, not all but some examples, are we doing enough with DHS? Is the partnership with the energy industry enough? Should we be doing something different -- I know it is not enough right now, but should we be doing something different that we are not currently doing?

Mr. Richberg. So CISA came out with cyber performance goals that NIST -- and I helped build this model back in 2014 -- the cybersecurity standard that we thought we were building as a template for government turned out to be something that the rest of the world and the private sector liked. They are using it.

So CISA has created cross-sector cyber performance goals, an on-ramp, an easy button for these low -- for individuals, small and medium businesses to say, "I am going to back into that model" without saying, "Oh, my goodness, I can do all of this."

Now CISA is building sector-specific cyber performance goals. So I would look for -- and I know the energy sector is starting to work on those. They are waiting to see where we and the IT sector go. They want us to be the pioneers but, yes, there is work to say, "We can come up with sector-specific ways of enhancing security that shouldn't be a heavy lift for the small players."

Mr. Pfluger. Hopefully, the collaboration continues to increase. Every energy company I meet with, I ask them, "Have you met with DHS; have they informed you of the threats; have they talked to you about your vulnerabilities?"

Mr. Johnson, we will go to you. Kind of switching gears, can you discuss what the basic firewall provides versus what cybersecurity tools are needed to secure school

networks properly? And you may have already answered this question, but --

Mr. Johnson. Well, thankfully there has been a lot of discussion about this in today's hearing. Thanks to all of you who led on this issue. I have three school-aged kids, so it is personal to me too.

I am thrilled about the proposal from the FCC to do the cyber pilot. The bottom line is I think it is a very good -- it is a very important step, and hopefully only a first step, to securing schools and libraries for our kids and their teachers.

Mr. Pfluger. In my district, San Angelo State University, they have got a public-private partnership there, a cybersecurity institute of excellence, and they have gone into the school districts there. Not only are they training, you know, college students, but they are also going into the school districts.

What would you tell universities like that to continue doing, and what would you tell them to do that they may not be?

Mr. Johnson. Well, I think things like that are a perfect example of just not leaving points on the field in terms of we have got the capabilities in these communities, and it is a matter of putting together schools, universities, other government institutions, a mix of local, State, Federal, private, academic.

Mr. Pfluger. How far behind are we versus the Chinese school-age children when it comes to these skills?

Mr. Johnson. That is funny. I think I -- I like our chances because our model, it is geared around dynamism, innovation. It is not as centralized, and that sometimes has some -- you know, creates some inefficiencies, but most of the time, overall, it creates efficiencies that can't exist in a centrally planned approach.

So I think I -- I don't know how you exactly would measure it, but I like our chances

in the long-term.

Mr. Pfluger. My time has expired. Thank you all.

Mr. Latta. Thank you.

The gentleman's time has expired, and the chair now recognizes the gentleman from Idaho's First District for 5 minutes of questions.

Mr. Fulcher. Thank you, Mr. Chairman.

And, to the panel, thank you for being here. It has been a long one and that, frankly, the issues that I was going to bring up have been brought up, but also some other things have popped in my mind that I would like to just ask you about.

Mr. Richberg, you have talked about power a number of times, and I can understand why that is the top of your 16. On this committee, smart grid is a frequent discussion and the benefits of smart grid when it comes to efficiency and those sorts of things.

But, from a cyber perspective, is having a smart grid in place better or worse? What I mean by that, is it more susceptible to cyber threat because there is more vulnerability points to it, or is it less susceptible because part of being the smart grid is being insulated from cyber attacks? Could you comment on that?

Mr. Richberg. Yeah. You have hit the crux. When we talk about vulnerability, we talk about the number of points of access, and that goes up exponentially when everybody is now feeding energy and data back into the grid. So that makes the problem exponentially worse.

To the extent that it is a homogenous system that everyone on the grid is using the same technology, that gives me one kind of problem to solve. That is good. And, if they can disconnect in realtime when something goes bad, that is also good.

But then one of my nightmare scenarios is, okay, because of the two-way flow of communications, if somehow you manage to not only cut off central power distribution but send something that tells the local to go to sleep, then I have made the problem worse.

So I look at it on balance and say I understand the efficiencies. I understand the good that can come of this. My sense is we still have undiscovered vulnerabilities, and security has a long way to go in fully meeting the requirements of a secure smart grid.

Mr. Fulcher. Thank you for that. So to that end, that brings up another question, and I am not sure who is best to address this to, but I am going to address this to Mr. Butler just because I have a sense that you might have a take on this.

Oftentimes in technology -- technology sector, the private market, private entities, are on the leading edge of that stuff, and government, Federal agencies, follow.

Do you see that in the area of cyber, and if so, what are some of the things that our Federal agencies can learn from the private sector that needs to be on our priority list in this area?

Mr. Butler. Thank you for the question, Representative Fulcher. I think that there has been a lot of discussion of partnership today, and certainly cybersecurity is an area where public-private partnerships are long running and active.

I think that a lot of the, you know, boots on the ground, threat analysis and research is happening at the companies that build the devices and software and services.

But I think that the National Cybersecurity Strategy recognizes that to this day, as we see from the conversation today, market forces alone in the U.S. have not been enough to push out insecure services and inadequate practices, in part because it is uncertain, right, who is going to be subject on any given day to an attack.

There is not a lot of certainty about who is going to be held responsible when an attack happens, and all of that goes, you know, upstream to the question of, for any given entity in the system, are we going to invest the resources up front to secure our systems, right?

Are we going to be able to spend money on that versus all the other things that, if you are a private company, your shareholders and investors want you to spend money on?

And there have to be both clarity and financial incentives to make those decisions tend towards the secure and resilient and away from the insecure.

Mr. Fulcher. Got it. Thank you for that.

I am out of my wheelhouse on this one in particular, but I am going to ask, Mr. Johnson, you can put me back in the right wheelhouse if I am way off.

But mid-band part of the spectrum, 1 to 6 gigahertz, seems to work pretty well for 5G because of the attributes there with the amount of data, long distance.

But it is my understanding that that spectrum is also used for control systems and some of the things that Mr. Richberg has been talking about -- power, medical systems and so on.

Is that true, and if so -- those are locally managed systems most of the time, with power and medical -- is that true, and if so, what can the Federal agencies better do to work with locals in that area.

Mr. Johnson. This literally is the subject of a -- that could be a whole hearing and was back in March. I think the bottom line is we have a need for more spectrum in commercial -- for commercial uses now than we ever have before.

It is going to create a crowding of the various spectrum bands, and we have to find

ways to maximize the spectrum availability because as we discussed in much greater depth back in March, if we have less commercial spectrum available than China does, for instance, which we do now in mid-band, that is going to lead to China's companies kind of dominating the supply chain, so we have to solve that.

Mr. Fulcher. Thank you. And I ran over my time, so I didn't give you enough there.

Mr. Chairman, I yield back.

Mr. Latta. Well, thank you very much. Seeing no other members wishing to be recognized, I want to thank our witnesses for being with us today, and I ask unanimous consent to insert into the record the documents included on the staff documents list.

Without objection, so ordered.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Latta. I remind members that they have 10 business days to submit questions for the record, and I ask the witnesses to respond to the questions promptly.

Members should submit their questions by the close of business on Friday, January 27 -- oh, I think we have one last Member coming in right on the gavel.

Mrs. Cammack. I am here. Woo.

Mr. Latta. Since the gentlelady from Florida's Second District is recognized -- or Third District, excuse me, is recognized for 5 minutes for questions.

Mrs. Cammack. Sorry. Stuck in a meeting with the Speaker. I apologize.

While I am booting my laptop or iPad up -- sorry -- literally ran. I will just start with you, Mr. Johnson. I wanted to talk to you about cloud -- the cloud and security surrounding the cloud.

Mr. Johnson. Great. I am very impressed with your commitment to cybersecurity.

Mrs. Cammack. We are trying. Just kidding. I am not going to talk to you about the cloud.

All right. So, Mr. Johnson, to reduce fragmentation and drive efficient collaboration between government and the private sector in cybersecurity, why would the focus not be through the individual sector-specific agencies as defined by Congress?

Mr. Johnson. I think those agencies are crucial, and that is just the beginning. But I think that is the beginning of something I talked about in my opening, the unique relationship the communication sector has, in particular, with the U.S. Government, going back before DHS even existed. That is the beginning of the collaboration that has to happen.

Mrs. Cammack. Well, I know that there is certainly a concern within industry about programs being mandated, right? And that has always been the concern of innovation being hampered and additional costs being incurred by sometimes erroneous regulations and red tape.

So I know in particular with the Internet of Things and the Trust Mark, there is a concern amongst people within industry that the program might not be voluntary, that in the future, we could see something grow.

So, Mr. Richardson, if you want to weigh in on that, as well as you, Mr. Johnson.

Mr. Richardson. Well, thank you very much, and my congratulations again on the sprint.

Yeah. From our organization's perspective, we are going to be bringing updates and improvements to cybersecurity regardless of what government does. It is a commitment of our members to improve the security of devices.

We think the notion of voluntary versus mandatory, just by way of looking at the likelihood of more companies to adopt it and bring it into the market, you are more likely with voluntary.

And that has been the experience, and that is what we have seen from several of our member companies. So, in that sense, that is, I think, basis for that point.

Mrs. Cammack. Okay. Thank you.

Mr. Johnson. And I would just add that the key here is performance and accountability. Sometimes, in some areas, a government mandate might help performance and accountability.

In others, and I think this IoT security, Cyber Trust Mark example is a great example. The other one I mentioned is the BGP internet routing scenario.

There are other ways of ensuring accountability that are, in some cases, more powerful, and most importantly, faster than a government process. So I think we can do that in IoT. It is going to create the standard for IoT security.

When the first Cyber Trust Mark is earned, it will -- I think it is going to revolutionize the market, and it is going to make that the reasonable security for enforcement purposes, for litigation purposes, for all sorts of market purposes. And you can do it faster. Same thing on BGP and collaborating on routing security.

Mrs. Cammack. Okay. I appreciate that. And I want to shift back into the cloud now. So how have cyber threats changed with the shift to cloud computing and network virtualization, if at all?

Should we, on this committee, focus on anything in particular in this space when dealing with the threat from the CCP and CCP-affiliated companies?

Mr. Johnson. That is also a very long question -- long answer. I think I will try to summarize by saying that cloud capabilities and virtualized networks -- for instance the way 5G operates as a virtualized network -- in most cases, promotes security.

And that is a much longer discussion, but it creates capabilities, intelligence capabilities, including AI threat detection that can exist in a different environment. So there is a major plus side to the virtualization of networks.

Where -- but it also creates new opportunities for bad actors to operate. So I think we should always be concerned about what the CCP and its intelligence agencies and proxies are trying to do, including in cloud. And there is a lot more to say about that.

Mrs. Cammack. We will have to talk offline about that.

Mr. Johnson. I am trying to talk faster than --

Mrs. Cammack. No, no, no, I appreciate it. And I am going to open this up to our entire panel. During my time at the United States Naval War College, when I was writing my thesis, I based my approach on the fact that there is a need to create a new service academy, the United States cyber academy, much in the way of the Naval Academy, the Air Force Academy, West Point, et cetera.

Because we are, at that time -- and I don't want to age or date myself, but at that time, we were about 9,700 official cyber warriors short. The concept being you can commission into military service or into Federal service because, as you all know, the university system tends to gobble up our most talented young people into private sector before we have an opportunity to actually see what they can do in the Federal sector.

Do you support the initiation and creation of a United States cyber academy to address this shortfall?

Mr. Johnson. You know, I think it is a great idea to explore. I don't know if I would be -- if I would want to say -- just give an easy yes or no now, but I think that type of capability, whether it is in the existing service academies or in its own standalone is exactly the type of thing we need.

Mr. Latta. You want to just ask for a quick, yes/no down the line?

Mrs. Cammack. Yeah.

Mr. Butler?

Mr. Butler. I don't have anything specific to add to that. I mean, I think that it is really important to address the workforce gap, and there is clearly a huge need, right, for expertise across sectors but in particular on the government side.

Mrs. Cammack. I am going to take that as a yes.

Mr. Richardson. I think I would echo what I have heard so far.

Mr. Richberg. I think the growing maturation of Cyber Command has changed that. The times when people in the MOS would go do it and then go do something dramatically different and come back, now I think I would be reluctant to say, "Break it off and have something separate."

I really think that it is part of combined arms. I think you learn better doing it in the existing Service academies and -- Cyber Command changes --

Mr. Latta. The gentlelady's time has expired.

Mrs. Cammack. I know I am way over my time. Thank you all, and we will talk offline. Thank you.

Mr. Chairman, I yield.

Mr. Latta. And, at this time, seeing no further members wishing to be recognized, I would like to thank our witnesses for being here today.

I also, once again, ask unanimous consent to insert into the record the documents included on the staff hearing documents list.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Latta. Without objection, that will be the order. Without objection, so ordered.

I remind members that they have 10 business days to submit questions for the record, and I ask the witnesses to respond to the questions promptly. Members should submit their questions by the close of business on Friday, January 26.

And again I want to thank our witnesses for being with us today and for your great testimony.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 12:56 p.m., the committee was adjourned.]