Preliminary Transcript

Diversified Reporting Services, Inc.

RPTS CARR

HIF201020

STOPPING DIGITAL THIEVES:

THE GROWING THREAT OF RANSOMWARE

TUESDAY, JULY 20, 2021

House of Representatives,

Subcommittee on Oversight and Investigations,

Committee on Energy and Commerce,

Washington, D.C.

The subcommittee met, pursuant to call, at 10:34 a.m., in Room 2123, Rayburn House Office Building, Hon. Diana DeGette, [chairwoman of the subcommittee] presiding.

Present: Representatives DeGette, Kuster, Rice, Schakowsky, Tonko, Ruiz, Peters, Schrier, Trahan, O'Halleran, Pallone (ex officio); Griffith, Burgess, McKinley, Dunn, Joyce, Palmer, and Rodgers (ex officio).

Also present: Representative McNerney.

Staff Present: Jeff Carroll, Staff Director; Austin Flack, Policy Analyst; Waverly Gordon, General Counsel; Tiffany Guarascio, Deputy Staff Director; Perry Hamilton, Deputy Chief Clerk; Rebekah Jones, Counsel; Zach Kahan, Deputy Director Outreach and Member Service; Chris Knauer, Oversight Staff Director; Kevin McAloon, Professional Staff Member; Will McAuliffe, Counsel; Jon Monger, Counsel; Kaitlyn Peel, Digital Director; Kylea Rogers, Staff Assistant; Andrew Souvall, Director of Communications, Outreach, and Member Services; Benjamin Tabor, Junior Professional Staff Member; Sarah Burke, Minority Deputy Staff Director; Marissa Gervasi, Minority Counsel, O&I; Nate Hodson, Minority Staff Director; Peter Kielty, Minority General Counsel; Emily King, Minority Member Services Director; Bijan Koohmaraie, Minority Chief Counsel; Clare Paoletta, Minority Policy Analyst, Health; Alan Slobodin, Minority Chief Investigative Counsel, O&I; Michael Taggart, Minority Policy Director.

*Ms. DeGette. The Subcommittee on Oversight and Investigations hearing will now come to order.

And I must say we are all extremely glad to be back in person. Welcome back to our in-person members, and welcome to our members who are here remotely.

Today our subcommittee is having a hearing called "Stopping Digital Thieves: The Growing Threat of Ransomware,'' and the hearing will examine the growing threats posed by ransomware to U.S. businesses and critical infrastructure, and we will discuss recommendations for combating those threats.

Due to the COVID-19 public health emergency, as I said, members can participate either in person or remotely. And if members are not vaccinated -- I think everybody here is, but if they are not, they must wear a mask and be socially distanced. They can remove their mask when they are recognized. And again, anyone else present in this committee room, including press, must wear a mask and be socially distanced or be vaccinated.

For members who are participating remotely, your microphones will be set on mute for the purposes of eliminating any background noise. Members participating remotely will need to unmute our microphone each time you wish to speak. Please note once you and your microphone, anything that is said in Webex will be heard over the loudspeakers in the committee room, and may -- and will be on

C-SPAN. So just -- we have experienced that some in the last few weeks, so just be aware.

Because members are participating from different locations, all recognition of members, such as for questions, will be in the order of subcommittee seniority.

And as always, if at any time during the hearing I am unable to chair the hearing, the vice chair of the subcommittee, Mr. Peters, will serve as chair until I am able to return.

Documents for the record can be sent to Austin Flack at the email address we have provided to staff. All documents will be entered into the record at the conclusion of the hearing.

And the chair will now recognize herself for the purposes of making an opening statement.

Today's hearing tackles a growing threat to our national security, economic security, and public safety, and that is ransomware. In short, a ransomware attack occurs when criminals break into a network, lock it down, steal data, and then extort everyday Americans into, often, massive ransom payments. These digital thieves are infiltrating our schools, hospitals, food suppliers, and critical infrastructure companies.

The seriousness of the issue is hard to overstate. All you need to do is to look at the front page of the newspaper to see the problem is getting worse. Earlier this year the

whole country watched as a single attack on Colonial Pipeline's information technology system shut down the gas and fuel supply to the entire Eastern Seaboard. This attack alone caused massive gas lines -- and many stations ran out of fuel.

Last year, more than 560 health care organizations, many of which were already reeling from COVID-19, found themselves victims of ransomware. Hospital systems had to cancel appointments and surgeries, reroute ambulances, and delay critical treatment for cancer patients.

Our food supply was also recently in the crosshairs when, a few weeks ago, cyber criminals attacked the company JBS, the largest meat producer in the world, threatening a vital link in our nation's food supply.

And these are just the attacks that we know about. Companies and organizations wanting to save face and maintain the confidence of the public often meet the ransom demands in secret -- always pay and hard to trace cryptocurrency. Like many -- or almost always doing that.

Like many of the issues we have examined in the last year-and-a-half, like vaccine confidence and the state of our public health infrastructure, the ransomware challenge is not new, but it has been exacerbated by the COVID-19 crisis. Cyber criminals thrive on exploiting vulnerabilities in our networks. The explosion of remote work and remote school during the pandemic greatly expanded these vulnerabilities.

For example, experts are projecting our K through 12 schools will face a nearly 90 percent increase in the number of ransomware attacks just this year. And it is not just the breadth of targets that is growing. The average size of ransom payments has also increased, reaching an estimated $312,000 per organization in 2020.

Simply put, the time to address this crisis is now. To win the fight we need not just a whole-of-government approach, but, really, a whole-of-society approach. Both the public and private sectors have a role to play.

First, the public sector must continue to develop and to lead a well-coordinated response. This includes coordination across U.S. Government agencies and private industry, and working closely with our international partners. With President Biden's recent actions we are seeing the outlines of such a response take place, and the Administration is rightfully treating the issue as a national security threat.

For example, our nation's first cyber director was sworn in just last week, and our Federal agencies are conducting a series of collaborations with the private sector to address ransomware and other critical cyber issues. I applaud the efforts that the Cybersecurity and Infrastructure Security Agency announced last week. That agency is working to ensure that small to medium-sized businesses across our country are -- that are victimized by ransomware attacks have the resources needed to minimize harm, and restart operations.

Internationally, it is imperative that countries no longer provide safe haven for these criminal organizations. And President Biden has vowed that America will take any necessary action to defend its people and its critical infrastructure. The President already addressed the international part of this issue head on, both at a G7 summit and in multiple one-on-one conversations with Russian President Vladimir Putin. And just yesterday, the U.S., along with our European Union and NATO allies, condemned China for its state-sponsored cyber activities, including ransomware attacks.

While the Administration's actions are promising, the public sector cannot defeat ransomware on its own. For example, following a ransomware attack, too often we hear of lax cybersecurity requirements or known vulnerabilities that were ignored. We have had a number of classified briefings where we heard about that. And it is critical that companies of all sizes address chronic under-investment in cyber defenses. Better cyber hygiene, more cyber expertise, and meaningful information-sharing will address this threat.

And Congress also has an important role to play in this. Just last week, key government cyber experts indicated that additional executive authorities may be needed to ensure the private sector gets to where it needs to be.

As a committee, we must ensure that the executive branch has the tools and authorities to mandate effective

cybersecurity requirements for vulnerable industries, modernize our defenses, and ensure that we are postured to compete with those threats. There is no shortage of policy proposals being discussed. Those include mandatory reporting of ransomware attacks, prohibitions on ransom payments, and increased regulation of critical industries and cybersecurities.

This morning, I want to say, we have a terrific panel of experts who have spent decades addressing ransomware and other cyber crimes, and I am really looking forward to hearing from all of you.

One thing is certain: this problem is not going away. The problem has grown exponentially over the last decade, and we must respond in kind. We must do everything we can to fix our vulnerabilities, and to protect our critical industries.

[The prepared statement of Ms. DeGette follows:]

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

*Ms. DeGette. And I want to thank all of you, and recognize our ranking member for five minutes for the purposes of an opening statement.

*Mr. Griffith. Thank you very much, Chair DeGette, for holding this hearing, and especially considering the recent increase in ransomware attacks across our nation, including high-profile attacks such as Kaseya, Colonial Pipeline, and SolarWinds.

I also want to thank the witnesses for taking your time to join us today.

Cybersecurity is integral to all organizations, and should be treated as a priority for maintaining the health and security of an organization, as well as any other individuals or entities that are affiliated with that organization. The need for more rigorous cybersecurity protections exists across all industries, including health care, oil, gas, water, and electricity. Any network with vulnerabilities can be subject to a cyber threat, and the frequency of cyber attacks is increasing exponentially.

The reach of most recent cyber attacks demonstrates how serious this issue is. For example, the Colonial Pipeline, one of the most critical pieces of energy infrastructure, was the target of a ransomware attack in May. The attack halted all pipeline operations, and caused supply disruption up and down the East Coast for over a week, which led to higher gas prices and longer lines. More recently, over the Fourth of

July holiday, Kaseya supply chain ransomware hack affected medium and small-sized businesses, globally, including in my district. Both of these attacks appear to be Russia-linked, which is the most recent showing of cyber threat Russia poses to the United States.

Although the recent attacks appear to be linked to Russia, adversaries of cyber attacks originate in different foreign nations, varying in the size of the criminal enterprises. And their approaches to gaining access to systems range in their level of sophistication.

However, no one industry or part of our nation's critical infrastructure is immune to the threats posed by these malicious actors. Cyber attacks have the potential to cause real harm, depending on the severity and the target. In health care in particular, direct harm is almost a certainty. Any time information in the -- in health care and public sector is compromised, it poses a risk to providers, patients, and those who serve and supply them.

But it is not just data and privacy that are compromised. Ransomware attacks can have a significant impact on patient health. For example, in May a ransomware attack hit a San Diego-based healthcare system, Scripps Health, and the cyber criminals stole data on close to 150,000 patients. This forced Scripps Health to not be fully up and running until a month after the cyber attack -- or cyber -- ransomware attack. These types of incidents are

detrimental to the care available to the community, and put a major strain on the surrounding healthcare system and the region. As the ransomware recovery timeframes increase from days to months, the amount of damages skyrockets. In a hospital's case, that can mean the difference between life and death.

The recent ransomware attacks are providing lessons about the importance of cybersecurity. These systems are fragile. Although it is impossible for a system to be completely resilient against any cyber attack, there is much more the Federal Government, cybersecurity organizations, cyber victim organizations, and the private sector can do to detect, respond, and recover from ransomware threats. This is a shared responsibility, and we need everyone to do their part.

The United States has great cyber experts found in both the Federal Government and the private sector that supply the key building blocks to revamping our nation's cybersecurity. The Federal Government has strong resources to prevent attacks, respond to attacks, and hold criminals accountable. We just need to see more of it, and we need to make better uses of our resources.

Coupled with the Federal government resources, we have private-sector firms that offer cybersecurity consulting for a range of organizations at different entry points in the cybersecurity cycles, and at different levels of

cybersecurity risk. Moreover, we have experts that focus exclusively on industrial control systems and operation technology cybersecurity. We also have nonprofit networks that design solutions for emerging threats, and private companies with specialized professionals to disrupt criminal enterprise.

We need to ensure an open line of communication, coordination, and information-sharing in the cyber world, and delineate proper responsibilities for developing cybersecurity strategies to the appropriate entities.

It is impossible to eliminate all cyber threats to our nation. However, we need to do more to better prevent and detect ransomware attacks, so that we can thwart the worst case outcomes and scenarios, especially when it comes to critical infrastructure.

I look forward to hearing from the witnesses here today, given their expertise and experiences in this space, and I am eager to learn more about what we can do to help prevent and detect future ransomware attacks.

I yield back. Thank you, Madam Chair.

[The prepared statement of Mr. Griffith follows:]

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

*Ms. DeGette. I thank the gentleman. The chair now recognizes the chairman of the full committee, Mr. Pallone, for five minutes.

*The Chairman. Thank you. Thank you, Chairwoman DeGette.

The Energy and Commerce Committee has a long history of examining cybersecurity on a bipartisan basis. Over the past several years we have held hearings on strengthening cybersecurity in the health care and energy sectors. We have also been regularly briefed by agencies on a variety of critical concerns related to both previous and recent cybersecurity threats and attacks. While we have made progress, it is clear much more needs to be done to address the ongoing threats we see nearly every day.

One area of particular and growing concern is ransomware, the topic of today's hearing. Ransomware is a malicious cyber security attack that paralyzes victim organizations. The attack freezes computer systems and holds data hostage until a ransom payment is received. Ransomware used to be considered a nuisance crime, impacting only an individual computer. But in recent years it has evolved to affect the entire networks of organizations, and even governments, extorting entities for enormous sums of money.

Increasingly, criminals deploying ransomware are not just freezing the data of victim organizations, but are also pilfering sensitive business and consumer data. On top of

locking down computer networks, they also threaten to release the stolen data as an additional method to leverage a ransom payment.

Just in the past few months we have seen a surge of ransomware attacks that, at times, have brought aspects of normal life and commerce to a standstill. The ransomware attack on the Colonial Pipeline disrupted oil and gas supplies on the Eastern Seaboard, causing many gas stations to run out of fuel, prices to skyrocket, and grounding air traffic. Other recent attacks have threatened local police departments, including the D.C. Metropolitan Police, and victimized schools, local governments, and hospitals already grappling with the COVID-19 pandemic.

I also want to underscore that the challenges brought on by these attacks are particularly acute for small businesses, many of which lack dedicated information technology staff and the resources, and are just trying to keep their businesses operating. And these victims may have no idea who to turn to if their data is subject to a ransomware attack. We simply can't leave victim organizations on their own in figuring out how to defend against and respond to these cyber criminals.

So given the huge scale and scope of these threats, I am pleased that President Biden is taking decisive steps to tackle this challenge. Just last week the Administration announced a new website, StopRansomware.gov, that is meant to provide a one-stop hub of ransomware resources for

individuals and businesses. The website outlines the simple steps small businesses can take to protect their networks, and provides guidance to these organizations on how to respond to ransomware incidents.

The President is also leading a whole-of-government effort to disrupt ransomware campaigns, and go after the criminals who launch them. The Administration strategy announced last week builds on an effort launched by the White House in May that will make it more difficult for criminals to transfer funds using cryptocurrency, helping make U.S. institutions more resistant to hacking, and urge international cooperation.

But the Biden Administration can't address this enormous challenge on its own. Congress must also take action, and that is why this oversight hearing is so important today. I look forward to hearing from our witnesses who have dedicated their careers to cybersecurity. They are uniquely positioned to make recommendations on the types of policies needed to defend against future attacks, and I am interested in their ideas as we explore potential solutions that will help further protect our nation's critical infrastructure networks, businesses, and consumers.

So with that, I thank the chairwoman for holding this hearing. I yield back, Madam Chair.

[The prepared statement of The Chairman follows:]

374 **********COMMITTEE INSERT**********

375

*Ms. DeGette. I thank the gentleman. The chair now recognizes the ranking member of the full committee, Mrs. Rodgers, for five minutes for an opening statement.

*Mrs. Rodgers. Thank you, Madam Chair. In recent months we have seen a significant increase in the ransomware attacks coming from Russia. In May, DarkSide, a ransomware group operating out of Russia, attacked the Colonial Pipeline, which accounts for about 45 percent of the East Coast's fuel. In June REvil, another ransomware group operating in Russia, attacked GBS (sic) USA, which temporarily knocked out plants that process roughly one-fifth of our nation's meat supply. Earlier this month REvil executed another ransomware attack, this time on American IT management software company Kaseya, which affected hundreds of businesses across the globe.

While Russian -- while the Russian President Putin may not be directly connected to these attacks, he refuses to crack down on them. White House Press Secretary Jen Psaki recently said that, "Responsible states do not harbor ransomware criminals.'' Well, Mr. President, Russia is not a responsible state, and greenlighting a pipeline for Putin after Russian cyber criminal attacks on one of the most critical pipelines in the United States certainly will not deter Russia.

But this threat is not unique to Russia. We know the Chinese Government engages in malicious cyber behavior, too.

Just yesterday the Biden Administration publicly blamed hackers affiliated with China's main intelligence service for a far-reaching cyber attack on Microsoft. While this Administration must do more, I applaud them for taking this step, and publicly addressing the threat China poses.

The White House also recently announced a cross-government task force to combat the rise in ransomware attacks. President Biden's nominee to lead the Cybersecurity and Infrastructure Security Agency, Jen Easterly, was also unanimously concerned -- confirmed, sorry. These are welcome steps.

I caution this Administration, though, and this Congress, from consolidating cyber at one agency. Doing so is a wrong and dangerous approach, because it weakens an agency's ability to leverage their expertise in cyber preparedness for their specific and unique sectors. I urge the Biden Administration to lean on that expertise.

Director Easterly, I urge you to rely on your colleagues at HHS, DOE, FCC, FTC, DOT, and others to address cyber threats in their sectors.

As the committee which oversees our economy's most critical sectors, we know, firsthand, the work of many of these Federal agencies around cyber. This committee itself has a history of working on cybersecurity issues to strengthen America's defenses against bad actors. The committee has conducted significant oversight over cyber

incidences dating back to Target, the Target hack in 2013 and 2017. We brought in the Equifax CEO to answer for the hack of their systems that resulted in the loss of 143 million Americans' personal information.

In 2018, following dozens of briefings, hearings, letters, reports, and roundtables, the Republicans on this committee issued a cybersecurity strategy report that provided specific priorities for more effective protection against vulnerabilities.

Earlier this year we sent bipartisan letters to the Department of Energy, the Department of Commerce, the Department of Health and Human Services, the Environmental Protection Agency, and the National Telecommunications and Information Administration following the SolarWinds attack.

Cyber threats and ransomware attacks will only continue to grow, and it is important for this committee to continue to lead on cyber issues. The Colonial Pipeline attack underscored the committee's long work to ensure the secure, reliable delivery of energy. The Pipeline and LNG Facility Cybersecurity Preparedness Act, reintroduced by Energy Subcommittee Republican Leader Upton and Chairman Rush, will provide DOE with strong, clear coordinating authorities to respond to future threats. And soon, our Consumer Protection and Commerce Subcommittee Republican leader, Gus Bilirakis, will introduce a bill to ensure the FTC is focused on ransomware attacks from abroad, and working with foreign law

enforcement agencies to hold those cyber criminals accountable.

Yet there is more to do. Energy and Commerce should continue to explore ways to identify and patch cybersecurity vulnerabilities before they are exploited. We should also encourage reporting by entities of cyber attacks to the Federal agencies who oversee them, and consider certain liability protections for our critical infrastructure. This is an important and timely discussion.

Thank you, Madam Chair. I look forward to hearing from our esteemed witnesses.

Thank you, everyone. I yield back

[The prepared statement of Mrs. Rodgers follows:]

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

*Ms. DeGette. The chair now asks unanimous consent that the members' written opening statements be made part of the record. And without objection, so ordered.

I now want to introduce our witnesses for today's hearing: Kemba Walden, who is the assistant general counsel for Microsoft Corporation; Robert M. Lee, who is the chief executive officer of Dragos; Dr. Christian Dameff, assistant professor of emergency medicine, biomedical informatics and computer science, University of California, San Diego, medical director of cybersecurity, UC San Diego Health -- we are not going to refer to that entire title every time we discuss it with you, but congratulations; Charles Carmakal, senior vice president and chief technology officer, FireEye-Mandiant; and Philip Reiner, chief executive officer, Institute for Security and Technology.

I want to thank all of you for appearing today, as I have said.

And I know you are aware the committee is holding an investigative hearing. And when doing so, we have the practice of taking testimony under oath. Does anyone here object to testifying under oath?

Let the record reflect the witnesses have responded no.

The chair will then advise you that, under the rules of the House and the rules of the committee, you are entitled to be accompanied by counsel. Does anyone request to be accompanied by counsel today?

Let the record reflect that the witnesses have responded no.

If you would, please rise and raise your right hand, so that you may be sworn in.

[Witnesses sworn.]

*Ms. DeGette. Let the record reflect that the witnesses have responded affirmatively.

Please be seated, and you are now under oath and subject to the penalties set forth in title 18, section 1001 of the U.S. Code.

The chair will now recognize our witnesses for a five-minute summary of their written statements.

There is a timer on the screen that will count down your time, and it will turn red when your five minutes have come to an end.

Let me first recognize Ms. Walden for five minutes.

TESTIMONY OF KEMBA WALDEN, ASSISTANT GENERAL COUNSEL, MICROSOFT CORPORATION; ROBERT M. LEE, CHIEF EXECUTIVE OFFICER, DRAGOS; CHRISTIAN DAMEFF, M.D., M.S., ASSISTANT PROFESSOR OF EMERGENCY MEDICINE, BIOMEDICAL INFORMATICS, AND COMPUTER SCIENCE (AFFILIATE), UNIVERSITY OF CALIFORNIA SAN DIEGO, MEDICAL DIRECTOR OF CYBERSECURITY, UC SAN DIEGO HEALTH; CHARLES CARMAKAL, SENIOR VICE PRESIDENT AND CHIEF TECHNICAL OFFICER, FIREEYE-MANDIANT; AND PHILIP REINER, CHIEF EXECUTIVE OFFICER, INSTITUTE FOR SECURITY AND TECHNOLOGY

TESTIMONY OF KEMBA WALDEN

*Ms. Walden. Chair DeGette, Ranking Member Griffith, and members of the subcommittee, thank you for the opportunity to testify today. My name is Kemba Walden, and I lead our ransomware analysis and disruption program within Microsoft's Digital Crimes Unit. Our unit is an international program of technical, legal, and business experts that has been fighting cyber crime to protect victims since 2008.

It is estimated that last year over 2,400 organizations were victims of ransomware attacks, with a financial impact of nearly half-a-billion dollars. I fear that we are only seeing the tip of the iceberg, as likely many attacks and corresponding losses go unreported. This recent proliferation of ransomware attacks impacts our national

security, our economic security, our public safety, and our health.

In my oral comments today I will focus on what ransomware is, how the ransomware process works. I also wanted to share some of the key trends Microsoft is observing.

So what is ransomware? Well, it is malicious software that, once deployed in a victim's network, locks that network and the information in it, making it inaccessible to the victim, unless the victim pays a ransom. You may have heard of different strains of ransomware, such as REvil and DarkSide, Conti, Ryuk, and so on. These are different types of ransomware, malicious software that lock a victim's network. Ransomware is installed after a series of criminal actions, so no single criminal gang is associated with any particular type of ransomware. It is simply the tool of choice for profit.

Today's ransomware attacks are different than the ones we experienced only a few years ago, where criminals deployed ransomware, often on a single computer in a predictable manner, and then demanded ransom in exchange for a decryption key to unlock that computer. Today's criminal has figured out how to use human intelligence and research to not only lock entire networks for a higher profit, but to commit double or, in some cases, triple extortion. We at Microsoft call this human-operated ransomware, otherwise known as big-

game ransomware.

Ransomware is a profitable business, with few barriers to entry. It takes no specialized skill to profit from this crime. Here's what we are seeing in recent cyber criminal attacks. They customize their attacks, and can be patient. Human-operated ransomware has evolved over the past few years, such that cyber criminals select specific networks to attack, and then hunt for entry vectors. Criminal gangs are performing massive, wide-ranging sweeps of the Internet, searching for vulnerable entry points, such as through unpatched software or successful phishing. Then they wait for a time that is advantageous to their purpose.

Because cyber criminals want to move laterally from one computer to the entire network, they focus on gaining access to highly-privileged account credentials. They have developed a modular business model that we refer to as ransomware as a service. A manager or ransomware developer will recruit affiliates who have collected access, or collected credentials, or otherwise specialize in some other crime, offering a cut of the profits or of an attack.

Make no mistake, these are fully-fledged criminal enterprises. They find opportunities to double or even triple-extort victims. So before locking down a victim's system, they will find high-value information and steal it. Not only will they demand payment to unlock a victim's network, they will demand payment in exchange for not leaking

the victim's data. In some cases, they will extort a victim a third time in exchange for not committing even more crimes, such as a DDos attack. They demand victims pay in cryptocurrency, thus taking advantage of the anonymous nature of this payment system.

While the movement of money is transparent, the crypto economy values privacy of the persons and the circumstances behind each transaction. So when cryptocurrency is used, criminals can easily verify when a victim has paid the ransom, but hide behind the opaqueness of a crypto wallet. Importantly, this blockchain technology does not cause cyber criminals to commit this crime. Rather, elements of the crypto ecosystem make payments a bit easier, facilitating the crime.

In fact, while working with the Ransomware Task Force, I learned that compliance stakeholders within the crypto economy are just as eager as anyone to eliminate the nefarious use of their platforms. So what do we do about it?

Well, there is something for everyone to do. The Ransomware Task Force Report does a great job laying this out, so I won't go into detail here. However, I want to underscore the importance of partnership and actional (sic) information sharing.

Criminals are smart, they are creative, they are well financed, and they are not limited by borders. The security community must match this. At Microsoft, our impact is

greatest when we work collaboratively with government and others in the private sector.

In conclusion, government has law enforcement and intelligence resources that private sector cannot match. The private sector has access to data and technological resources that governments cannot match. We must work together to find innovative solutions.

Thank you, and I look forward to your questions.

[The prepared statement of Ms. Walden follows:]

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

*Ms. DeGette. Thank you so much.

Now I am now pleased to recognize you, Mr. Lee, for five minutes.

TESTIMONY OF ROBERT M. LEE

*Mr. Lee. Thank you. Chairwoman DeGette, Ranking Member Griffith, and members of the committee, thank you for providing me the opportunity to testify before you today.

I started my career as an Air Force officer, and spent most of that time tasked at the National Security Agency, where I built and led a first-of-its-kind mission to hunt for and analyze threats targeting industrial control systems. At that time, cyber threats towards industrial systems were seen as a possibility, but not as a reality.

The problem, though, is everyone was looking in the wrong location. Analysts around the community were hunting for threats in enterprise IT, or information technology, networks, such as those that people depend on for personal computer usage and email. What we were not doing is looking at industrial and operations networks themselves, such as those in power plants, pipelines, water utilities, and manufacturing sites. Broadly, I will refer to this as operations technology, or OT.

The easiest way to explain OT is to consider that everything we have in IT, plus physics. When adversaries target IT networks, they often steal data. And when they disrupt them with malicious software such as ransomware, it impacts workers' ability to do their job. When adversaries target OT networks, they can, intentionally or not, create

unsafe conditions that cause damage to the world around us, up to and including the loss of human life.

As I mentioned, though, we did not see the various OT threats that existed, because the broader community was looking for OT threats in IT networks. We lacked the visibility in OT to determine what was happening. In essence, we had the equivalence of Schrodinger's OT. We did not look inside the box to determine if the cat was alive or not. In my time at the NSA we started looking inside that box. To our surprise, we found a wide variety of state actors targeting these systems.

Today, at Dragos, we track 15 state actors targeting OT around the world, including many operations in the United States. Specific to the topic of ransomware, we have responded to numerous incidents and ransomware incidents in OT. Each company has done the right thing; they have sought out help. However, these incidents happen far more often than people realize. Across all the cases, though, we continue to see that a lack of visibility in the OT networks leads companies to believing that they are in a better place than they actually are.

Our hearing today, appropriately, is on ransomware. But I want to underscore that it is just one risk facing our infrastructure and, if anything, highlights that, if criminals can be successful in breaching and disrupting our networks, state actors will find much more success.

However, the threats are worse than we realize, but not as bad as we want to imagine. And ultimately, defense is doable. Today I want to highlight a few key points.

Number, to defend against ransomware, we must first find a way to harmonize the roles and responsibilities of the private sector with government.

Number two, there must be a simplified, unburdened process and single point of contact with the government. CISA, as an example, could be the front door of government, who could then coordinate the interagency and communicate clearly to the private sector. There are recommendations in the National Infrastructure Advisory Council and Cyberspace Solarium Commission to improve analyst collaboration, as well.

Ransomware in OT, my third point, is exposing the under-investment in cybersecurity in many organizations. My prediction is, as we look to counter the ransomware threat, we will start to gain more insights, and those insights will lead us to find more state actors and other threats. We must be prepared for what we find, and think about the ransomware strategy as an overall portion of our cybersecurity strategy.

Number four, critical infrastructure companies stand ready to do the right thing and partner with government fully. However, differing regulation regimes and requirements can distract from the focus. Whatever regulations and standards manifest, they should be thought of

together, so that companies do not have overly burdensome requirements on them as we all try to achieve the same goal.

And lastly, government should communicate the why and the what to the private sector, but leave the how to the experts in those entities. We have seen this work very well.

This Administration and the Department of Energy launched a 100-day action plan earlier this year focused on OT. They did that in the electric sector. The goal was increasing real-time information-sharing, visibility, detection, and response capabilities in OT networks. The government laid out the requirements, and why they wanted companies to do this, but they did not dictate the solution or how they had to achieve it. This was done in collaboration with the electric sector leaders, as well.

The electric sector coordinated, evaluated what was on the market, and chose Neighborhood Keeper, a technology made by Dragos, in collaboration with the Department of Energy. They then deployed it quickly, voluntarily, and at their own costs. As a result, we went from less than 5 percent of the electric system monitored in the United States to more than 70 percent of the electric system monitored in OT networks in under 100 days. This is the exact type of visibility and success useful in preventing ransomware and those issues.

Government setting requirements and amplifying them is important. Letting the private sector figure out innovative ways in how to achieve those requirements is paramount. I

thank the committee for providing me the opportunity to testify today, and welcome any additional questions or information.

[The prepared statement of Mr. Lee follows:]

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

*Ms. DeGette. Thank you so much.

Dr. Dameff, I am now pleased to recognize you for five minutes.

TESTIMONY OF CHRISTIAN DAMEFF

*Dr. Dameff. Madam Chair DeGette, Ranking Member Griffith, distinguished members of the subcommittee, thank you for this opportunity to speak today on the effects of ransomware on health care. My name is Dr. Christian Dameff, and I am a practicing emergency medicine physician. I am also an assistant professor of emergency medicine, biomedical informatics, and computer science at the University of California, San Diego. I also serve as the medical director of cybersecurity for UC San Diego Health, the first position of its kind in the United States.

Early in my adolescence, my fascination with computers and networks led me to the hacker community, who taught me to appreciate the complexity and fragility of modern computer systems. Today I use that knowledge to improve the cybersecurity of health care. My research focuses on the patient safety and care quality impacts of cyber attacks. At my core, I am an emergency medicine doctor. I am trained to care for any patient who comes through the door, whether they suffer trauma, heart attacks, strokes, or COVID. I am here to tell you that health care is not prepared to defend or respond against ransomware threats.

Our hospitals today are increasingly dependent on technology. Doctors admit patients into the hospital, order and review laboratory tests, prescribe medications, and

prepare for surgeries, all while using computerized workflows. We have come to implicitly trust and rely on these systems. And when they fail, health care grinds to a near halt.

We know ransomware attacks affecting the health care sector are increasing in frequency, sophistication, and disruptive potential, in addition to the exposure of sensitive data, severe financial losses, and reputational damage. A cyber attack on a hospital has the potential to threaten life and limb.

When patients suffer from strokes, heart attacks, or severe infections, minutes matter. The best outcome for patients with these time-dependent crises depend on immediate, continuous availability of the same digital systems that ransomware can disrupt. When critical medical systems go offline, our opportunity to save lives diminishes. The risk of error or misdiagnosis increases. We are now learning that cyber attacks impact not just the infected hospitals, but the surrounding healthcare ecosystem at large.

Two months ago, a ransomware attack disabled five large hospitals in the San Diego area for an entire month. Adjacent hospitals were quickly overwhelmed with unprecedented numbers of emergency room patients, many of whom had serious time-dependent illness. Wait times skyrocketed. Hospital beds rapidly filled. Clinicians caring for very sick patients lacked vital medical records

from the infected hospitals. I saw firsthand the spillover effects, and understood that the vulnerability of one hospital is a vulnerability of many hospitals.

You have heard today from experts with technical and policy recommendations that, if enacted, would improve ransomware defenses across all sectors. However, I hope you now understand that health care has unique challenges, and necessitates additional actions.

First, the effects of ransomware attacks on patients' health should be scientifically studied. Most hospitals are not currently equipped to measure or report the impacts of these attacks. I recommend the development of standardized metrics of cyber attack severity on hospitals. Mandatory reporting of patient safety and care quality outcomes should occur for severe attacks. I recommend that Federal agencies such as the National Institutes of Health and the National Science Foundation prioritize funding for research on this topic.

Second, identifying cybersecurity vulnerabilities before they are exploited will protect patients. There is currently disparity between what I call the health care cybersecurity haves and have nots. Lesser-resourced, critical access, and rural hospitals need help when it comes to increasing their preparedness. As we seek to protect vulnerable hospitals, we must also avoid overly punitive measures for those who are unfortunate enough to fall victim to highly complex or novel

cyber attacks, understanding that stiff fines or penalties may worsen an already devastating operational impact. We are only as strong as our least-defended communities.

Third, I support software bill of materials as one mechanism to increase transparency around cybersecurity vulnerabilities. Software bill of materials enables manufacturers and health care delivery organizations to take more proactive steps to manage their cybersecurity risk.

Furthermore, I recommend ongoing support and legal protections for security researchers engaging in good faith security research, otherwise known as coordinated vulnerability disclosure. We need help from ethical hackers if we are going to defend against the malicious ones.

Lastly, we must prepare hospitals for inevitable attack. The ability to rapidly deploy backup manual patient care systems is key to reducing patient harm. Such contingency planning takes resources and expertise.

In conclusion, I applaud this committee's leadership on ransomware response, and remain optimistic about improving cyber resilience in health care. Our patients deserve excellent care. Ransomware and other cyber attacks targeting hospitals threaten our ability to deliver that care as it is needed, when minutes matter.

Thank you for this opportunity to testify today, and I welcome any questions you may have.

[The prepared statement of Dr. Dameff follows:]

852

853 **********COMMITTEE INSERT**********

854

*Ms. DeGette. Thank you so much.

The chair now recognizes Mr. Carmakal for five minutes.

TESTIMONY OF CHARLES CARMAKAL

*Mr. Carmakal. Thank you. Chairman DeGette, Ranking Member Griffith, and members of the subcommittee, thank you for this opportunity to share our observations on the ransomware threat. My name is Charles Carmakal, and I am a senior vice president and CTO at Mandiant.

Mediant is an organization that helps other organizations across the globe deal with incredible cybersecurity challenges. We have got over 1,000 security professionals within 25-plus countries that help organizations deal with a variety of threats, including those threats that are orchestrated by foreign governments and organized criminals.

My colleagues here have done a pretty good job of talking about the ransomware overview, but I would like to provide a little bit more details on what the problem is like today. Ransomware is the number-one cybersecurity threat that we all face today. But what the -- the problem that we are dealing with today is much more than just ransomware.

We call the problem "multifaceted extortion.'' This is how organizations get compromised by threat actors, and they deal with types of attacks where threat actors will steal data from organizations, disrupt business operations, will embarrass those organizations. They will reach out to partners of those organizations and extort them. They will

reach out to customers and extort them, thus applying pressure to the victim organizations to pay substantial extortion demands. Extortion demands often will range, sometimes, starting in six figures. But very often, for larger organizations, it could turn into seven figures, or even eight-figure demands.

Unfortunately, we work with organizations that are compelled to pay substantial extortion demands, not because they want to, not because they feel like that is the best option, because they really have no choice.

We work with organizations to really think about what are the things that they need to consider before paying extortion demands. I would like to share some of the observations and the learnings that we have acquired working with thousands of organizations dealing with this type of threat.

I think there is a lot of misconceptions about why threat -- why victims pay threat actors. I think there is an assumption that organizations that have to pay don't have good cybersecurity hygiene, or they don't have good backups in place. And let me just dispel a few myths. A lot of times we find victim organizations pay threat actors because they want to accelerate the process of recovering their business operations. If you think about a situation where a municipality loses access to their emergency services, or a hospital can no longer treat patients and have to divert

patients to other hospitals, it becomes incredibly important to get access to systems as quickly as possible. And so we sometimes find that victim organizations feel compelled to pay, because they feel that it is quicker to pay and to recover systems than it is by just using their backup infrastructure.

We also find that backup infrastructure generally isn't resilient enough to restore every single computer that was impacted over a short period of time during a ransomware and a multifaceted extortion operation.

The second thing that organizations need to think about before paying is how reliable is the threat actor. And I know it sounds kind of silly, thinking about the reliability of a threat actor, but today we find that a lot of criminals, they do demonstrate a certain level of reliability because they have recognized their business model actually depends on that.

You also need to understand whether or not the threat actors stole data from the organization before deploying decrypters -- or before deploying encrypters across the enterprise. And if they stole data, there is obviously the risk of publishing that information. And we find that many victim organizations choose to pay because they feel that it is in their best interest to protect the sensitivity and the privacy of their customers and their business partners' information from being exposed on the Internet.

The next thing that organizations need to think about is does the threat actor still have active access to the environment, and, if they do, can they escalate their attack and conduct more disruption?

You also need to understand whether or not cyber insurance will cover the claim.

And finally, you really need to think about is the threat actor sanctioned by the United States Government, and is it actually legal to pay the threat actor?

So those are some of the considerations that we talk to our clients about. And it is always our clients' decisions as to whether or not they should pay or not. But we want to actually walk them through the considerations.

So let me actually share some of the observations that we have learned when victims have actually paid threat actors.

Well, first of all, you can't just pay a threat actor and hope they go away. Technically, they have multiple different back doors to get access back into the environment if they want to. Many times we do find that they tend to move on, and move on to the next victim. They don't tend to come back, once they are paid, but technically, they do have the ability to do that.

You don't know who you are paying. You have no idea if you are paying a sanctioned entity. You have no idea if you are paying a terrorist organization. You don't know who you

are paying. It is typically a responsibility of a separate company that engages in the negotiations with a threat actor and actual facilitation of payment. And a lot of times they are the ones that are actually trying to figure out who is being paid. But at the end of the day, you never know who is actually getting the money.

As I mentioned before, many threat actors are actually reliable because, again, they are -- their business model depends on it. Reliability certainly, you know, depends on who the threat actor is. Many times we find that threat actors will provide working tools to be able to recover your systems and data. And they also provide a promise to delete the data that they have stolen from the victim environment. Of course, you never actually have any real guarantees that the data was actually deleted that was stolen from the victim environment.

We do anticipate, at some point in time, that some of the data that was stolen -- and for those threat actors that were paid, we do anticipate that they will likely publish information and the stolen data at a later point in time, especially as time goes on.

In conclusion, I would like to thank you for this opportunity to testify before the subcommittee. The ransomware and the multifaceted problem has become at a level that is completely intolerable, and we need to come together as a community to better address the problem. Thank you.

[The prepared statement of Mr. Carmakal follows:]

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

*Ms. DeGette. Thank you so much.

The chair now recognizes Mr. Reiner for five minutes.

TESTIMONY OF PHILIP REINER

*Mr. Reiner. Madam Chair DeGette, Ranking Member Griffith, Chairman Pallone, members of the subcommittee, thank you for the opportunity to testify today on the pervasive threat that ransomware poses to our national security. My name is Philip Reiner, and I am the chief executive officer of the Institute for Security and Technology.

Our mission at IST is to create trusted venues where national security policymakers can engage with technology leaders to work together to devise solutions to emerging security threats. That is what allowed us to convene the Ransomware Task Force, of which I was the executive director. We were pleased to convene representatives from more than 60 public and private organizations to devise a comprehensive framework for combating the ransomware threat.

I will focus my testimony here today on three areas: first, on the top-line recommendations of that task force report; second, note, some positive steps we have seen taken since that report launched in April; and third, note some items from the report that will require congressional action.

As is often repeated, there is no single solution to this challenge. It poses too large of a threat for any one entity to address alone. The timing of this hearing is thus incredibly important. This is an international cybersecurity

crisis, the scale and magnitude of which demands leadership and action. The task force determined four goals that should frame a comprehensive approach to deter, disrupt, prepare, and respond. These goals are interlocking and mutually reinforcing. This framework should be considered as a whole. To achieve these goals, the priority recommended actions were as follows.

Number one, coordinated international diplomatic and law enforcement efforts must prioritize ransomware, and work to eliminate criminal safe havens.

Number two, the United States should and must lead by example, and execute a sustained, aggressive whole-of-government, intelligence-driven anti-ransomware campaign, coordinated by the White House, and in close collaboration with the private sector.

Number three, governments should establish cyber response and recovery funds; mandate that organizations report ransom payment; and require organizations to consider alternatives first, before making any such payments.

Number four, a clear, accessible framework must be developed to help organizations prepare for and respond to ransomware attacks.

And then number five, the cryptocurrency sector must be better understood, and more closely regulated to prevent further facilitation of ransomware.

Since April, encouraging actions have been taken, some

of which have been noted already. These include the recent White House launch of an interagency ransomware task force. This is a critical initial step, as the United States needs to execute a campaign that leverages all tools of national power: diplomatic, economic, intelligence, law enforcement, and military. Again, this must be done in close cooperation with the private sector in order to be successful.

Additionally, the call for leader-level diplomatic prioritization of these issues, in some ways, has been heated. President Biden has repeatedly asserted that ransomware is a top priority, and included this as a top-three item in his recent summit with Russian President Putin. Similar prioritization by the United Kingdom, the G7, the EU, Australia, and others continues this necessary trend. These declarations are great initial steps, and need to be followed up on with action. DOJ and DHS have their own internal ransomware-focused efforts. The National Institute of Standards and Technology has released an initial ransomware profile. Also, seven large U.S.-based insurers have established a consortium to share data. Follow-through will be the key for all of these steps and, hopefully, for many more that are to come.

Finally, a number of recommended steps from the report can be highlighted that necessitate congressional action, which include, but are not limited to, requiring organizations to report ransomware payment information prior

to payment; requiring further steps to shore up the cryptocurrency ecosystem; providing clarification of lawful defensive measures that private-sector actors can take; requiring local governments and managed service providers to adopt limited baseline security measures; and creating a ransomware response fund to help incentivize the non-payment of ransoms.

Congress has a critical role to play in a whole-of-government response to this threat, and the Institute for Security and Technology welcomes the opportunity to inform the work of this committee. Thank you for your leadership, and I look forward to your questions.

[The prepared statement of Mr. Reiner follows:]

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

*Ms. DeGette. Thank you so much, and thank you to the entire witness panel for excellent testimony. It is now time for our questioning, and the chair will recognize herself for five minutes.

As I said in my opening statement, senior cyber experts from the government have expressed concern about some of the private sector's compliance with cyber hygiene requirements, and the limits of --

*Voice. This meeting is being recorded.

*Ms. DeGette. Thank you. And the limits of the Federal Government's existing authorities to manage the problem.

So, as Congress, it is our job to make sure that the executive branch has the authorities it needs. I want to hear from each one of you about this.

Mr. Reiner, your testimony identifies eight priority considerations for Congress. Which two or three of those would be the most impactful, and why?

*Mr. Reiner. Madam Chair, thank you for the question. I appreciate the sentiment that there is much more that companies can be doing. I think --

*Ms. DeGette. Sir, I have five minutes. So if you can tell me which two or three of the actions you identify would be most impactful, I think that would be helpful.

*Mr. Reiner. Yes, ma'am.

*Ms. DeGette. Thank you.

*Mr. Reiner. As the report laid out, I think one of the

steps that can be taken for organizations, as part of potential grants that can be provided, that they need to expand a certain percentage of their efforts on cybersecurity, to basically raise their baseline application of their own funds in order to receive national grants.

Another element that the task force put forward was that, in order to receive grant funding, was that a company would have to meet the baseline requirements that are put forward in the framework that we described in the report, that NIST put forward --

*Ms. DeGette. So -- but basically, what you are saying is tie government grants to good hygiene.

*Mr. Reiner. Yes, ma'am.

*Ms. DeGette. Ms. Walden, I wanted to ask you, your testimony cites a Microsoft study which estimates "more than 99 percent of cyber attacks would have been prevented if multifactor identification were deployed.'' So do you think that we should mandate basic cyber hygiene requirements through legislation? And if so, which ones?

*Ms. Walden. Thank you, Chair. Yes, so we published a report that 99 percent of cybersecurity attacks would not have happened without -- because of multifactor authentication. So I think that you should encourage basic cyber hygiene principles like multi --

*Ms. DeGette. Do you think we should mandate it?

*Ms. Walden. I think I agree that we should require it,

yes.

*Ms. DeGette. Ok, thank you.

*Ms. Walden. Yes.

*Ms. DeGette. Now, Mr. Lee, in your testimony you seem to agree that additional cybersecurity requirements could be helpful, but cautioned that we shouldn't be regulating the "how.'' Can you explain very briefly what you mean by that?

What do you think the most effective legislative or regulatory requirements would look like?

*Mr. Lee. Absolutely, thank you. Generally speaking, we need to be more outcomes-driven. And so a lot of times companies will be told, "You must install antivirus,'' "You must do the patching within seven days,'' or whatever that kind of prescriptive requirement is. But across our different infrastructure, especially in our operations side of the house, things can be so varied. And we need to tell them what are we actually trying to solve for.

*Ms. DeGette. Okay --

*Mr. Lee. We want you to be able to respond this quickly, or so forth.

*Ms. DeGette. To be results-oriented.

Mr. Carmakal, your testimony cites to a white paper published by Mandiant that outlines the priority technical actions companies should take, ideally, prior to a ransomware event. And I am wondering if you have seen widespread adoption of those recommendations. And if not, what can we

do to help companies implement those actions?

*Mr. Carmakal. Thank you, Chairwoman. So we basically built that white paper as a documentation of the playbook that we use when we conduct incident response exercises. And so these are the types of things that we recommend to organizations after a breach. But certainly, those could be applied beforehand.

Unfortunately, not enough organizations are taking that knowledge and applying it within the organizations. We would love to see greater adoption. Unfortunately, a lot of the things that we see day-in/day-out, from a response perspective, shows that they --

*Ms. DeGette. So what can we do to either encourage or mandate them to --

*Mr. Carmakal. I would certainly love for more encouragement of organizations to try to learn from other breached entities. And that white paper is a good example of those learnings.

I don't know that I would necessarily say that you need to mandate it, but more encouragement --

*Ms. DeGette. But Mr. Reiner has a good suggestion, though, which is to tie it to government grants. So you need to meet a certain standard if you are going to get your public funding. What do you think of that idea?

*Mr. Carmakal. Generally, I think that sounds like a good idea.

*Ms. DeGette. Great. Finally, Dr. Dameff, as a medical doctor and cyber researcher, you have an interesting perspective to share. I am wondering if you can talk if there are specific issues in the health care industry, and what this committee -- we have jurisdiction over health care policy -- what we can do to ensure good cyber compliance. Briefly.

*Dr. Dameff. Thank you, Madam Chair. One of the most important things I can articulate today is the need for additional information. It is very difficult to measure the impacts of a cyber attack on a patient. In other industries you can measure the cost in dollars and cents. That is immediately understandable. Or downtimes resulting in increased gas prices. But in health care we do not have the infrastructure in place to get the basic data, to measure what happens to our patients.

And what really matters is whether or not they walk or talk after a stroke, or whether or not they survive after a heart attack. Without measuring those very basic things through things like NIH funding, scientific inquiry, we don't even know the magnitude of the problem or the impact on our patients.

*Ms. DeGette. Thank you. The chair now will recognize Ranking Member Griffith for the purposes of asking questions for five minutes.

*Mr. Griffith. All right, Dr. Dameff, and this is not

on my list of questions, but it came up as a part of feeding off of Chairman DeGette's questions.

Ms. Walden said, you know, we could have prevented a lot of these hacks with multifactor identification. You are an emergency room doctor. How is that going to work? Because it is easy to say here, but how is it going to work in your emergency room?

*Dr. Dameff. That is a great, great insight. Thank you for the question. There are technical controls that will definitely improve the cybersecurity posture of hospitals. Those should be employed, right? Many hospitals are deploying multifactor authentication, or already have, for protecting patient data.

You identify a key element here, which is that patient care cannot be hindered in the emergency sense by overly -- over-security controls that impact patient care. I will say this, though. It is not necessarily about which controls can prevent the infection. Honestly, I am of the belief that we should prepare for an inevitable attack, and then have a backup system in place to restore patient care as quickly as possible, and rely on that until you can restore that. That is how you save lives. That is what you do, is focus on your immediate response to restoring patient care, while those technological systems come back online.

*Mr. Griffith. All right. So my next question would be how expensive is that going to be?

And let me give you a reason why I am concerned about this. I represent a large rural district. In a portion of my district the previously competing hospital chains, for financial reasons, were forced to merge, and they were given clearance by both state of Virginia, the Federal Government, and the State of Tennessee to basically have a monopoly in that area. So I have got one hospital system serving many counties in east Tennessee and southwest Virginia. How expensive is it going to be for them, because they are under financial stress already, to set up this good hygiene?

And do they -- how are we going to fix that? I mean, how expensive is what you are talking about? Because, in this case, should what happened in San Diego happen there, there are no hospitals to send these folks to that aren't at least an hour to an hour-and-a-half away, maybe further than that for some of the folks. What are we going to do? Help me.

*Dr. Dameff. Again, thank you for that fantastic question. The consolidation of health care, exactly as you mentioned, has increased the risk to patient safety from ransomware attacks because of the shared infrastructure and technology among many hospitals in a specific geographic location. We have seen that. That is what happened two months ago, is that a single health care delivery organization that was infected; five hospitals in a geographic location were devastated. That exactly would

impact patient care, potentially.

And your identification of critical-access hospitals as being a target, potentially, of attack, as well as the patient harm implications cannot be overstated.

Specifically how are they going to afford this? Really, two things. One, that disaster resiliency that I mentioned before, restoring technical systems in the background, but having a manual, non-technical process to take care of patients in the meantime, that already exists at most hospitals. That is emergency response. That is disaster medicine. They prepare for earthquakes and hurricanes, and have plans in place to do that. They should enact that -- or they should prepare for that in a cyber context.

The second thing is that is true, it is going to be costly for a lot of the technical controls, and there are hospitals out there that cannot afford it. They will simply not be able to. I worked at hospitals and took care of COVID patients in resource-stricken hospitals, wherein they were concerned they were going to run out of ventilators. How do we expect them to be able to defend against cyber attackers, and spend millions of dollars, potentially, to increase their cybersecurity posture?

It is going to require some creative solutions. Quite frankly, I don't see any --

*Mr. Griffith. So what you are saying is that is a problem we are going to have to solve.

*Dr. Dameff. Yes, I think that is going to be a big, big problem you have to solve.

*Mr. Griffith. I appreciate that, and I tend to be tight with Federal dollars, but this may be one area we don't have any choice.

Let me say also, for us to provide assistance to an organization, we need to know in advance, or we need to know when it happens, if they are being attacked. And of course, there are many reasons for not telling us. And you and Mr. Carmakal want to -- might want to tag-team on this one, if I have time -- I am running out.

But particularly related to hospitals, should we be looking at, if not mandating, having a minimum requirement that would then give the hospitals some protection? If they have done their cyber – the good cyber hygiene to a minimal requirement that perhaps the Federal Government sets up or industry sets up, that they would then be limited on liability in any suits that might follow, where a patient's health was affected, do you think that is -- that idea would work?

*Dr. Dameff. I am definitely in support of ways we can incentivize, instead of slowly penalize hospitals for trying to take care of patients. That is really key. Perhaps tying it to reimbursement, for example, wherein if you meet a certain cybersecurity threshold of protections, you can see increased reimbursements for some of your medical care as a

way to incentivize. I could see that as one potential mechanism where we can achieve even the most rural and critical access hospitals achieving the appropriate amount of cybersecurity protections.

*Mr. Griffith. All right, and if Madam Chair will give me just the patience for a second, Ms. Walden, if you can get to me in writing later, what do we do about cryptocurrencies, and its involvement in all of this?

Just -- if you can cite me some articles later, or whatever, and we will probably send you a written question on that, as well, and I yield back.

*Ms. Walden. I am happy to.

[The information follows:]

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

*Ms. DeGette. I thank the gentleman. The chair now recognizes the full committee chairman, Mr. Pallone, for five minutes.

*The Chairman. Thank you, Chairwoman DeGette. One of my concerns is that ransomware is a very sophisticated form of attack, and it is not clear to me that smaller companies and, to some extent, even larger companies have the resources or tools needed to deal with these threats. So I was pleased to see the StopRansomware.gov website that was launched by the Biden Administration last week, and -- because it provides a new resource hub for small businesses and other organizations.

But I mean, that is a good start, but I am wondering if we can and should be doing more to assist U.S. companies, particularly small to medium-sized businesses, to deal with these threats. So let me start with Mr. Carmakal.

Given your experience in incident response, can you explain the types of resources that companies need, once they find themselves in the midst of a ransomware attack?

*Mr. Carmakal. Yes, absolutely. Unfortunately, a lot of these small organizations, some of them, don't even have security staffs. Some of them rely on IT resources to perform security functionality.

When I think back to October of 2020, when we saw an acute problem against health care organizations, I talked to a lot of hospitals that were taken offline, couldn't take

care of patients leveraging digital technology. They ended up having to divert patients to other hospitals. And I ended up talking to the IT resources, who were trying to desperately get their systems back online. They didn't know anything about digital forensics. They didn't know anything about threat actors. They didn't know how to respond to the intrusions. And so it was a very difficult situation for those organizations to face, and I really do feel, for a lot of the smaller organizations that don't have dedicated security teams.

So, look, to the extent possible I want organizations to do the best that they can, from a, you know, cyber hygiene perspective. But I don't believe the onus is fully on the organizations themselves. I think there is a shared responsibility --

*The Chairman. Well, what kind of resources would they need is what I am asking.

*Mr. Carmakal. Yes, I think they would need -- well, I think they would need government support. And, from a government support perspective, I think there are things that government could do in terms of indictments, arrests of individuals that are behind these attacks.

I think there is more information-sharing that could occur for victim organizations that could be applicable to other organizations out there.

I think there are, you know, things in terms of

disruption that government can do to curb the problem of ransomware, so that these smaller organizations that don't have the resources and the staff have some additional government support.

*The Chairman. But I guess -- and let me go to Mr. Reiner – I know that there is, you know, law enforcement agencies that assist, and a lot of what Mr. Carmakal mentioned relates to that. But are we providing -- are there a variety of resources beyond just, you know, the traditional -- or some of the law enforcement, you know, such as technical expertise that the government can or should be providing, or can the government provide help in assessing the scope of their situation?

I know he discussed some of that, but if you would respond also, Mr. Reiner.

*Mr. Reiner. Yes, Mr. Chairman. I think, through the process that we conducted for the Ransomware Task Force, I mean, there was an array -- really, a list of things that we put forward that we believe could be done to get ahead of this, right? So to get to the left of boom, so that you better equip companies to be able to defend themselves.

As has been discussed, though, a lot of those organizations really don't have the capability to do so. So CISA and other departments and agencies, I believe, can be very well positioned to help share that information, provide those tools in advance for free. But folks don't know about

it. They are not even aware that it exists. So how do you get it to them?

Awareness campaigns are often belittled as not effective enough, and not quick, but there needs -- there can be a lot more to get the information out there that there are tools that are available. StopRansomware.gov, for example, great idea, fantastic amalgamation of government resources. How do you tell people that that is something that they can turn to and utilize?

I think there is one piece here that is incredibly important that came up over and over again through the process that we conducted, which was that departments and agencies that are responsible for doing this don't have the resources that they need in order to develop those tools to engage those private-sector partners to actually get that word out. NIST, DHS, other departments -- Commerce, other departments and agencies really could use buttressing of resources, so that the folks who are really specifically responsible for that training and that piece of it have more capacity to do so.

*The Chairman. Okay. Just quickly, Ms. Walden, when you talk about cyber security -- I mean cryptocurrency, I am sorry -- again, I don't think the small business owner knows much about how to purchase or trade that. So how do you see -- in other words, if a small business is faced with having to pay ransom, for example, in cryptocurrency, how likely is

it they are going to be able to navigate that? And what resources would they need?

There is only 20 seconds left, but if you could just comment.

*Ms. Walden. Well, first, hopefully, small business would opt not to pay the ransom.

*The Chairman. Right.

*Ms. Walden. But if they chose to pay the ransom, the criminal actors are actually quite helpful. They have a bit of customer service. Their ransomware notes will instruct the victim on how to or where to obtain, usually, Bitcoin, because Bitcoin is a lot easier to obtain than other types of cryptocurrency. But there are avenues for small businesses to be able to obtain cryptocurrency.

*The Chairman. Your recommendation is don't pay, though, sure.

*Ms. Walden. But my recommendation is do not pay.

[Laughter.]

*The Chairman. Right, thanks a lot. Take care.

*Ms. DeGette. I thank the gentleman. The chair now recognizes Mr. Burgess for five minutes.

*Mr. Burgess. I thank the chair, and I thank our panel for being here today.

It is, obviously, not the first hearing we have had on this. It is a little remarkable to me that we don't have law enforcement as part of the panel, however. It has come up in

previous panel discussions that law enforcement can only go after people that they know they need to go after. And it has also come up in the past that there are disincentives to report.

Dr. Dameff, you have kind of mentioned that it could be -- the reputational damage can be significant from your hospital or hospital network.

In the past I have wondered if the construction of the Office of Civil Rights, the data breach reporting that was created as part of the HITECH Act back in 2009, if this is a disincentive to reporting. Once a company becomes listed, or once a health care entity becomes listed on that, it is -- they are, essentially, archived forever. And I have wondered if we should have a statute of limitations, or a statute of repose, or some remedial actions that can be taken by an organization that would allow them to extricate themselves from that list. Is that something that has come up in any of your discussions? For anyone on the panel.

Dr. Dameff, I will just ask you specifically, since you work in a hospital.

*Dr. Dameff. Thank you. The question of whether or not reporting record breaches -- as part of their mandatory reporting, whether or not that inhibits potential reporting of ransomware impacts, I think is still unknown. I will say, anecdotally speaking, I could see how that would prevent individual organizations from wishing to report, or perhaps

delay the impact of the reporting until they are -- to anticipate what might potentially be a large punitive fine.

There also -- when a hospital is hit with ransomware, they are also trying to restore operational capacity to take care of patients.

*Mr. Burgess. Yes.

*Dr. Dameff. And there are so many competing things happening at that exact moment, it is difficult to then report.

*Mr. Burgess. Let me ask you about that, because you brought that up. And we have spent a lot of time in this subcommittee and other subcommittees talking during the pandemic about the Strategic National Stockpile. Of course, the creation of the Strategic National Stockpile was in an emergent situation. You could deliver a set of things to an institution that they would need to function in whatever the emergency -- earthquake, hurricane, flood.

So is it possible to have an urgent deliverable of what you would need to run your -- say, your emergency room at your hospital, if you were just completely shut down with a ransomware attack? Is that something that we should look at?

*Dr. Dameff. I definitely agree it is something we should look into.

One of my recommendations is coming up with metrics to measure the impact to a hospital. And hospitals that have severe attacks that would be devastating to patient care

might benefit from such a resource, akin to something like the FEMA DMAT response, in which --

*Mr. Burgess. Right.

*Dr. Dameff. -- outside resources, personnel, systems, tents, et cetera, could be deployed rapidly to help alleviate those patient care constraints, while they are restoring systems. It is definitely something that should be looked into. We have never seen anything like that before.

*Mr. Burgess. So at this point we don't even know -- if there is a major hospital system that gets attacked, we don't know, downstream, is there a loss of life, was there -- as you pointed out, during the course of treatment of a stroke, is there a loss of function that could have been preserved? We just don't know the answer to those questions, do we?

*Dr. Dameff. And that is why I recommend in my testimony here that there be mandatory reporting for severe attacks on patient safety implications.

One of the barriers to that is that systems in which we measure care quality and patient safety are themselves targets of the ransomware.

What do I mean? The way that we measure the quality about a stroke care or a heart attack or something else is measured and recorded in the electronic health record. The electronic health record is ransomed.

*Mr. Burgess. Yes.

*Dr. Dameff. So we don't even have tools to measure

that, because they are also collateral damage from the actual attack.

*Mr. Burgess. Let me ask you this. And, you know, in order to get the proper metrics, in order to get the proper -- be able -- for us to make proper decisions, you are going to have to get proper information. It is hard to get proper information if people are scared to report.

You and I -- I am a physician, also -- we live in the world of the National Practitioner Data Bank, right? There is a central location that a hospital credentialing committee can query as to whether or not we have had a problem in other cities, and we are just taking our problems from town to town. Do you think there would be a benefit from having something structured along the lines of a National Practitioner Data Bank for data breaches, for ransomware attacks?

*Dr. Dameff. Forgive me, for individual physicians or for health care delivery organizations?

*Mr. Burgess. For the health care organization, writ large.

*Dr. Dameff. I do believe that we should get visibility on the differences in organizations that are under attack. But to penalize them, or to fine them significantly would reduce their ability to bounce back from that attack, deliver care. And so, whether or not it should be like a National Provider Data Base but for health care ransomware attacks, I

would support any efforts that collect additional metrics on ransomware attacks, and to make that data transparent and public.

*Mr. Burgess. Yes, the difficulty there is, though, when we get -- then you drive -- you are driving a fear factor: I don't want to report, because I don't want to be included.

*Ms. DeGette. The gentleman's time has expired. The chair now recognizes --

*Mr. Burgess. I am going to send you some questions in writing on that, as well as other members of the panel.

[The information follows:]

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

*Mr. Burgess. I appreciate you --

*Ms. DeGette. The chair now recognizes Ms. Kuster for five minutes.

*Ms. Kuster. Thank you very much, Chair DeGette. I appreciate you holding this hearing today.

Today's discussion regarding ransomware attacks and the growing threats that they pose presents a unique opportunity for this subcommittee to identify existing vulnerabilities and gather information on actions Congress can take to respond to this emerging threat.

As we have heard today, ransomware attacks are not new, but they are certainly increasing in number and sophistication in recent years. We continue to see front page news reports on this attack, but it is not just the high-profile ones that are occurring. The implications of these attacks have a far-reaching effect beyond the companies that are being targeted.

The attack on Colonial Pipeline's information technology system a few months ago had a significant disruption in energy distribution on the entire East Coast that led to delivery delays for businesses, and gas stations closed for over millions of Americans. This is just one example of why we need to explore what makes these companies vulnerable to begin with, and what they can do about it.

Ms. Walden, you state your testimony that "applying basic cybersecurity hygiene can prevent a cyber criminal's

ability to ransom a system.'' For the benefit of the business owners who may be watching this hearing, Ms. Walden, what are the most common vulnerabilities that put companies at risk of a ransomware attack?

*Ms. Walden. Thank you for the question. Yes, that is true. You -- the best way to resolve a ransomware is to make sure that it can't get into the system in the first place.

So there are some simple things that are just true for preventing cyber attacks in general: enabling multifactor authentication; doing better training of your employees and staff on identifying phishing and preventing the click; segmenting your network -- and those are tools for CISOs to take, but segmenting your network so that cyber criminals, once they are in, can't laterally move. But these are some of the simple cyber hygiene activities that small and medium businesses can and should take to prevent ransomware or any other cyber criminal attack.

*Ms. Kuster. Thank you. And I know, as Members of Congress, we are learning to do our best in that regard, as well.

It is clear that companies need to be giving increased attention to cybersecurity. But the amount of threats and vulnerabilities can be overwhelming. Mr. Carmakal, if you were running a medium-sized company, what are two or three things that you would do right away, across the board to protect your systems and data?

*Mr. Carmakal. Yes, thank you, ma'am. Great question. There is a few things I would do.

Number one, to the best of my ability, I would try to enable multifactor authentication on all remote access into my organization.

Number two, I would try to educate my employees as best as they can to identify phishing emails. But I do need to recognize that employees will always fall victim to phishing emails at some point in time, so I need to provide technology to block as many of those malicious emails as possible, and also provide technology and processes so that, if something does get past the initial security system, we have got other checks and balances to be able to identify the attack as it occurs.

The third thing I would do is try to, to the best of my ability, install all the security patches that I can and that I know about across my environment.

*Ms. Kuster. Very helpful, thank you.

I note that some cybersecurity measures are very expensive, especially if they involve reconfiguring entire networks, but the cost of these attacks is also increasing. Mr. Reiner, is it fair to say that investments in cybersecurity are good returns on investment?

And what more can be done to incentivize companies to make these changes, or spread the word about the necessity of addressing vulnerabilities?

*Mr. Reiner. You know -- thank you for the question. As we have spoken about extensively as part of the Ransomware Task Force, is that -- investing in this up front is much more affordable than having to, as you describe, having to reconstitute your entire organization after an attack. So absolutely, putting the investment up front in order to stay left of boom and make sure that these are not attacks that can actually get into your system, is absolutely where folks should be putting their resources.

I think the thing that can be reverted back to a little bit is what we were talking about before, which is getting the information out to those folks who don't really have the resources. One of the things that we delved into was in this spectrum of organizations there are companies that know, that have resources, but choose not to invest. How do you help inform their decision-making, so that they choose to do so? You incentivize them through some of the steps that we have spoken about here today, tying grant making, relieving penalties if they are compliant, et cetera.

I think there are organizations out there, though, that simply do not know that this is happening, and they do not have the resources in order to prepare in advance. We have to do better, I think, in terms of getting to them and letting them know what it is that they can be doing better.

Everything that was just described, multifactor authentication, et cetera, those are simple things that folks

can be considering. We need to get that information to them --

*Ms. Kuster. Sorry to cut you off --

*Ms. DeGette. The gentlelady --

*Ms. Kuster. I need to yield back. Thank you.

*Ms. DeGette. The chair now recognizes Mrs. Rodgers for five minutes.

*Mrs. Rodgers. Thank you, Madam Chair.

Earlier this year Scripps Health was hit with a ransomware attack. In the attack the cyber criminals stole data on about 150,000 patients, and caused significant disruptions in operations. A family member of mine -- or a family member of, really, a constituent of mine -- was directly affected by this attack, and so I have heard firsthand how devastating it was, and the impact on their health. The Scripps attack is a stark reminder of the stakes of cybersecurity. When the hospitals are hit, it can, literally, be life or death.

Mr. Dameff, these attacks can have a direct impact on patient health and outcomes. Can you help us better understand the cyber threat hospitals face today, and provide a few examples of situations where a patient's health was negatively impacted by a cybersecurity or ransomware attack?

*Dr. Dameff. Thank you. It is true that, in some medical conditions, minutes matter. For example, we have sometimes minutes to hours to treat a stroke, wherein our

medications and our treatments will no longer benefit that patient after a certain amount of time. The same is true for things like certain heart attacks. And our ability to diagnose a patient is tied to the technology that we use every day, as clinicians, that technology we are so dependent on.

So you can imagine, during a large ransomware attack, wherein these technical systems are no longer available, that we can't do our jobs, as clinicians. I jokingly say I am the generation of doctors that has never used paper records. Until early on in my fellowship training I had never had written a prescription.

The future of health care is not going back to the days of antiquated systems. In the future, we are only more technologically tied to our systems that we use. That -- when it is not there, we can't do our jobs well enough. It takes longer to get test results, to make decisions to give things like antibiotics in severe infections, or to identify when patients have certain conditions.

So you can imagine at that -- at a scale of not just one or two patients, but of a -- you know, 5 or 6 or 10 hospitals down at once, where you could imagine that would impact care along the continuum, not just patients in the emergency department, patients in clinics, patients in the ICU, patients that are in ambulances that have to be transported longer distances because hospitals under attack are on

diversion. These are all examples of how patients could potentially be impacted by this.

I will say, though, we do not have the ability to measure that impact. As mentioned previously, the systems in which we measure care quality and patient safety, themselves, are digital, are affected by the ransomware attacks. So I fear we don't even have the tools now to answer that basic question.

Furthermore, I would say that these types of attacks are exceptionally chaotic, and there is a lot of things happening at once. The ability for hospitals to report on that type of thing is nearly impossible as they attempt to restore their systems.

*Mrs. Rodgers. Okay. As a follow-up, you have expertise in the field of medicine and cybersecurity. In your opinion, what steps should hospitals take to better secure their networks against cyber attacks?

*Dr. Dameff. I think it is shared among many of the panel, the same types of technical controls: multifactor authentication, focusing on rigorous backup, and restorations. But there is -- my number-one recommendation would be to prepare for an inevitable ransomware attack, to practice and prepare for taking care of patients without systems, and to be able to do that at -- within two or three hours of an attack.

There are a lot of hospitals in this country that have

not considered this type of attack on their systems, have not prepared adequately for it, have not put in place how to take care of 1,000 patients without technology. That is the number-one thing I would encourage most hospitals across the country to do now. There is a framework for that at every hospital. And that type of preparation, at least in its beginning, doesn't cost a dime.

*Mrs. Rodgers. Thank you.

Ms. Walden, what are the ways the private sector can partner with government to address ransomware attacks?

*Ms. Walden. Thank you for that question. The government has legal authorities that the private sector doesn't have, right? They have law enforcement authorities, they have intelligence authorities. The private sector, frankly, has a lot of signals. But if you match those things together, we can do coordinated actions to bring cyber criminals to justice.

So law enforcement can bring the criminal to justice. Private sector can work along with law enforcement to identify those criminals. But we can also work with law enforcement to tear down the infrastructure that they use.

*Mrs. Rodgers. So what do you believe we need to be doing, as far as coordinating between the two, then?

*Ms. Walden. I believe that we need -- and I know I keep saying it over and over again, but we need actionable information sharing. I like to be able to exchange ideas and

signals and technology with my government partners to be able to get at the problem together.

*Mrs. Rodgers. So how are we doing?

*Ms. Walden. From the digital crimes perspective, we have great relationships with all of U.S. law enforcement, but we also have great relationships with other countries and their law enforcement. I think this Administration is taking the -- cyber crime and cybersecurity seriously, and they are signaling the right things, the right messages to would-be cyber criminals, and cyber criminals across the globe. And I think working with our allies is working pretty well. There is still a lot to do, but I think we have taken the best first step that we can.

*Mrs. Rodgers. Okay, thank you. I yield back.

*Ms. DeGette. I thank the gentlelady. The chair now recognizes Miss Rice for five minutes.

*Miss Rice. Thank you, Madam Chair.

Mr. Carmakal, can you speak more about ransom payments, and how we should be treating them?

And, you know, you talked a little bit about what the motivation is to pay them or not to pay them. Can you just expand on that a little bit?

*Mr. Carmakal. Yes, absolutely. Thank you for the question, ma'am.

So, look, most organizations, they don't want to pay an extortion demand. They just feel that they have no other

option. And, you know, for whatever reason, you know, maybe they feel like they need to accelerate the process of being able to recover their business operations, or perhaps they feel like they are doing the right thing to minimize the impact to their customers, or to their partners, or to maybe the intellectual property that they have, where they don't want that information to be published on the Internet for anybody to be able to download.

And so, you know, I have had an evolving position on ransom payments. Many years ago I was in the camp of, absolutely, you never want to pay an extortion demand, because we all grew up learning that, and we all grew up understanding you don't pay criminals, you --

*Miss Rice. Yes.

*Mr. Carmakal. -- don't give in to terrorist demands.

But what I have learned is, over the years, many of my clients, against my recommendations, made payments, and they actually saw relatively positive outcomes. They got access to their data, or perhaps they paid because they didn't want that information that was stolen to get published on the Internet.

And so I recognize that there are certain situations in which a company may choose to pay, and they might get some temporary benefit out of it. It is not necessarily going to be a long-term benefit. So the temporary benefit may be companies get access to their systems and data through the

decryption tools that are provided by the threat actors. The potential long-term benefit is that the data that was stolen may never end up being published on the Internet.

But again, there is no guarantees that things won't show up down the road. And I do anticipate, over time, we will start to see threat actors that have been paid will end up publishing the data at some point down the road. And that was a pretty common thing, prior to 2019, for us to observe.

*Miss Rice. Mr. Reiner, that kind of brings me to one of the issues that you have raised, which is the need to understand and regulate cryptocurrency. Can you talk more about what we can do here, as a body, in that area?

*Mr. Reiner. Thank you for the question. It was a pillar of the conversations that we engaged in, as part of the of the Ransomware Task Force. This is a major facilitating element of what really has accelerated what we are dealing with, in terms of the ransomware threat today.

The -- from my perspective -- and it really has been a learning experience for me to better understand specifically what are the choke points when it comes to cryptocurrency, the ecosystem. Where exactly can we focus our efforts to try and make it so that criminals cannot abuse these systems?

These are incredibly innovative capabilities. I think that is a separate conversation.

What can we actually do, though? We can work much more closely with the community that understands these systems,

and how they work, and get into the weeds as to how they are being abused. I do not think that that is very clearly and well understood broadly within government, but also in the private sector. And I think that would afford a great deal of opportunities, if we have that sort of information exchange and transparency, and understand it. You will see more clearly where it is that we can do more to stop criminal abuse of those payment systems. It is an incredibly complex web, because so much of it is really outside of jurisdictions.

So there is this notion that we came up -- or that was often noted in the process, this jurisdictional arbitrage. The United States is not alone in this effort. We have partners internationally that we can work very closely with, who have the ability to do things that we can't.

*Miss Rice. Well, who is doing it right?

And, I mean, I think you mentioned that the -- for Federal agencies that have jurisdiction over this issue --

*Mr. Reiner. Yes.

*Miss Rice. Is it a resource issue? Is it an intellectual capacity issue? Are we not able to hire the best and the brightest? What -- where is the deficit?

*Mr. Reiner. I would argue, from the -- so from where I sit, we see a wide variety of technologies that disrupt various elements of our society. This is a technological ecosystem that is very disruptive, and it is incredibly

innovative, and we are just behind the curve. We haven't -- really quite yet understood what it -- how it works, and how to get ahead of that, from a policy perspective. I think the policy is really playing catch-up here.

There are folks, I think, who are out there that can be relied upon, as Ms. Walden noted earlier, who are interested in playing a role to make sure that they are -- they don't want their systems being abused. They want to be seen as legitimate, and they are willing to engage in these conversations. Is a conversation that we need to engender, though.

To your question of who is doing it well, I think there is a lot of work that still needs to be done. Internationally, I don't know that there really is one that I would point to that is really doing it well yet. I think there is a lot of growth that we need to see happen there. But we can help lead on that effort, from the United States.

*Miss Rice. Thank you very much.

*Ms. DeGette. I thank the gentlelady. The chair now recognizes Mr. McKinley for five minutes.

*Mr. McKinley. Thank you, Chairwoman DeGette. Thank you for the panel.

I am a little frustrated that you all have put together a lot of efforts to try to help out and guide us, but even Johnny Wooden used to say there is some confusion over efforts versus accomplishments. And I am frustrated over the

lack of accomplishments, because our U.S. laws on cyber crime were originated in 1987. And then our last international cyber agreement originated in 2001. So cyber criminals are exploiting these outdated laws, clearly, and they are targeting our critical infrastructure, as we have all talked about here, so far with it.

And it is not just in America. Just in the last 2 years we have seen a 500 percent increase in ransomware attacks, and a 300 percent increase in the amount of money that is being exchanged with this.

So I looked back on the history of it since we have been chatting about this, these efforts. In the Ukraine, Russia attacked Ukraine in 2015 and 2016, and tried to destabilize their country. The Mexican oil company has been attacked, Pemex, by ransomware. The oil fields in Saudi Arabia were hacked by Iran in a retaliatory move. And then earlier this year, the water system in Florida was attacked. So -- and then what you have heard also is the Colonial Pipeline. It was held for a ransom payment. And we understand, as was noted earlier, it provides oil for half the East Coast in this. And we saw the consequences. We saw increased prices and shortages with it.

Yet these attacks on our critical infrastructure certainly, I think, could be mitigated with updated reforms to our international treaty, including some stiff, enforceable penalties. But -- and also -- and I believe it

was you, Mr. Carmakal, was talking about cryptocurrency, understanding and getting control over cryptocurrency.

But -- so what I am saying to you, as an alternative, while you all work your magic and efforts, what about an accomplishment -- if we could develop a redundancy in our energy system, a backup system?

For example, earlier this year Texas suffered massive outages after an electric generation failure. It could have been avoided if they had had the ability to go backup, to connect to their neighboring states, to get electricity. This lack of redundancy in their electric grid has served as a, to me, a stark reminder as an alternative to avoiding problems like this.

So -- but President Biden, and his people on the left, unfortunately, seem to be continuing to block this optional exchange of building additional pipelines as a redundant system. In this report that was just printed back in May, it talks about how this environmental council is not recommending any creation, maintenance, or expansion of pipelines in America. That is going to make us more vulnerable, to where hackers can get into our system.

We look at the Keystone pipeline, Line 5 in Michigan; Williams Pipeline in New York; the Atlantic coastline, the Mountain Valley Pipeline, all in West Virginia, all were part of our critical national security, are under attack or have been canceled with it.

So even Tom Seagal, in 2015, came before our committee, and he said that he could hand pick 10 engineers at Berkeley, and those 10 engineers, within just a matter of a few days, could shut down -- 4 days, he said -- in 4 days could develop a system to shut down our electric grid between Boston and New York. That was testimony for our office. So we know these hacks are going to occur.

But what we need -- what I am looking for is how do we develop -- while the magic is developing, how do we deal with it?

What are -- how do we develop redundancy on this?

So my question to all of you is would a reliable firewall -- while a firewall was being developed, or your systems being developed, would you support development of a redundant energy system for additional pipelines, so that if we do get hacked, we can go around it to -- and we -- I think it would lessen the attractiveness of attacking our pipelines, if we could do a redundant backup system. Would you support that, any of you?

I will start with you -- I want to call you dammit, but I know that is not right.

*Dr. Dameff. I would support any efforts to increase health care resiliency in the face of cyber attack, broadly. It is quite difficult to build redundant hospitals, for example. But there are --

*Mr. McKinley. I am talking about energy. I am

primarily talking about energy. I will let the other people on this committee to deal with some of the other matters. But I think on energy, I think, our national security is at risk.

I have run out of time, so I yield back. Thank you.

*Ms. DeGette. I thank the gentleman. The chair now recognizes Ms. Schakowsky for five minutes.

*Ms. Schakowsky. So this has been pretty frustrating, actually, and I hear remarks like we are playing catch-up, that it is -- the cyber criminals are getting more and more sophisticated, and it does feel like we are -- we have a lot of catching up to do.

And I also heard that there is no one, internationally, that is necessarily doing better than we are.

As a part of a legislative body -- and I do believe that Chairman DeGette did ask the question -- are there things that come to mind now, where we, as a legislative body -- for example, I chair a subcommittee of the Energy and Commerce Committee that deals with consumer protection, and I am wondering if we should be thinking about or getting your advice on legislation that might address the problem that we are facing.

I understand that it is totally multifaceted, that the executive branch has a huge role to play here, that it is beginning to do more of that. But can you advise us on the kinds of things that we could play?

I -- really, anybody can jump in. You are looking, you know, ready to go.

*Mr. Carmakal. I would love to take your question, ma'am.

*Ms. Schakowsky. Mr. Carmakal? Okay.

*Mr. Carmakal. So, first of all, look, I am equally frustrated about the problem. Every week it is exhausting for incident responders to have to deal with highly disruptive attacks against organizations. And it feels like every week it gets worse and worse.

But I do want to take a moment to celebrate the wins, because there has been a lot of wins out there, and I don't think we always celebrate that, or we don't celebrate it enough.

Number one, I think organizations are defending themselves against attacks every single day. We may not talk about that publicly, but it happens a lot.

Number two, I would like to --

*Ms. Schakowsky. Let me just ask. Do you think there should be any requirements for building in these security systems?

*Mr. Carmakal. I think there is a general expectation for most organizations to have cybersecurity controls and resiliency in place. Whether that is enforced by law, or there is -- generally expected by customers, I think that does exist.

*Ms. Schakowsky. Go ahead.

*Mr. Carmakal. Beyond that, I think there is a number of wins. If you look at some of the things that government has been able to do over the past few weeks and months -- and I am pretty proud and excited that the bureau was able to recover some of the funds that were paid by Colonial Pipeline to the threat actors. That was a pretty big win. And it is exciting to be able to see some of those actions taking place.

It is pretty exciting to see some of the disruption to threat actor botnets like TrickBot and Emotet, and some of the more nefarious botnets that are operating out there, and that is a good example of public-private collaboration and coordination.

*Ms. Schakowsky. Well, I --

*Mr. Carmakal. Just this week --

*Ms. Schakowsky. I want to just interrupt for a second.

*Mr. Carmakal. Yes.

*Ms. Schakowsky. And then where does responsibility mainly lie?

Should the Federal Government be required, then, to step in if there has been a failure in security that should have been considered by the -- either the private sector, or --

*Mr. Carmakal. I think there is a shared responsibility from victim organizations, from security companies, from government. I don't think any one party can handle the

problem on their own. It is going to require a concerted effort from multiple different parties, and I think we all need to step up, and we all need to celebrate the wins, and we need to actually continue to emphasize effort on the wins, on the things that have been happening successfully.

And I look at things that the FBI is doing in terms of notifying victim organizations about upcoming intrusions. It is incredibly powerful when that happens, when somebody from the FBI calls a victim organization and says, "There is a threat actor in your network today, and if you don't do something about it in the next three days, they are going to take your business offline.'' A lot of times that victim organization actually has the ability to call in for help, and to disrupt the threat actors and eradicate them from the environment.

So when we see actions like that from the government, I mean, it is incredible. You look at what happened earlier this week, or yesterday, with the indictments of a number of, you know, Chinese individuals that conducted intrusions over the past several years. Those indictments are good steps. They are good tools in the government's capability to try to curb the problem. So we would love to see much more of that happening.

*Ms. Schakowsky. Thank you.

Ms. Walden, you said, "Don't pay,'' that -- so what is the alternative to that?

*Ms. Walden. Well, I think there are a few things that can take place, and that Congress can do in order to prepare the country and to raise the maturity level of potential victims, and one is to create a recovery fund of some sort so that victims aren't alone in absorbing --

*Ms. Schakowsky. Could you turn on your microphone?

*Ms. Walden. Sorry, is that better?

*Ms. Schakowsky. Yes.

*Ms. Walden. Ah, sorry about that. A couple of things that Congress can do to make sure that victims are at a maturity level to be able to not pay, right?

So one of those things, for example, is raising the baseline for cyber hygiene, bringing everybody to a cybersecurity maturity level that can handle it.

Another would be to develop a cost recovery fund that will allow -- that will help victims absorb -- and the country, really -- to absorb the cost of critical infrastructure for having down operations.

On the cryptocurrency piece, if I may, it is helpful to know which department or agency has authority over the crypto economy, whether it is -- and the investors, right? Whether it is the SEC or the CFTC, that is a great start.

So I also want to make a shameless plug for the Ransomware Task Force report. I think there are about a dozen or so potential legislative actions recommended in there.

*Ms. Schakowsky. Well, why don't -- I would like --

*Ms. DeGette. I am sorry --

*Ms. Schakowsky. -- to see those.

*Ms. DeGette. -- the gentlelady's --

*Ms. Schakowsky. And I yield back, I am sorry. Thank you.

*Ms. DeGette. That is okay. The chair now recognizes Mr. Dunn for five minutes.

*Mr. Dunn. Thank you very much, Madam Chair, and thank our panel.

You know, recent ransomware and other cyber attacks have highlighted our vulnerabilities, showing the difficulties in holding those who perpetrate these attacks accountable. And it should not escape any of us that the vast majority of these significant cyber attacks originate from within countries that just happen to be our greatest foreign adversaries: Russia and China. It is my belief that the best defense is a good offense, and that goes for ransomware, as well. You know, we have to put Russia and China on notice that they will be held accountable for these organizations operating freely in their company.

So, you know, I think back to the 2014 OPM hack. It put millions of Americans' records risk, tens of millions. This was something, you know, that Congress and the American Government simply has to address.

With that, Dr. Dameff, there has been a significant

uptick in ransomware attacks on health care organizations, certainly since 2016. Now, I was amused when you said you had never written a note in a chart, you had always -- EMRs. You know, I actually go back to the days when we had a lot of paper, and we got a lot of work done. So I would say, while technology -- and, you know, it certainly has made huge, you know, advantages in medicine -- I am concerned that we are not ready for cyber attacks. Is there a single vulnerability that you would point to that makes us -- that is worse than any of our other vulnerabilities in health care?

*Dr. Dameff. Thank you so much for that question. If I could point to a single one, it is at the heart of what you mentioned, which was this hyper connectivity that was accelerated over the last 11 or so years by meaningful use. The thought we would digitize health care rapidly to improve care --

*Mr. Dunn. Everything is connected to everything.

*Dr. Dameff. Yes, and I think the commensurate security required for that did not happen, and did not occur. And so we are in a position now where we have a very difficult sector, generally a soft target for cyber attacks and ransomware.

And then, on top of that, we have a lot of demands, especially over the last year. The COVID pandemic has spread thin many health care delivery organizations across this country and across the world. And as a consequence, they are

left juggling many different constraints, of which only cybersecurity is one of them.

*Mr. Dunn. Yes, and I would dare say that we are not paying as much attention to cybersecurity as we were before the pandemic. Everybody is a little tired, I appreciate that.

In the interest of time, I am going to switch gears a bit here. You know, the U.S. Government confirmed just yesterday a mass ransomware attack on Microsoft earlier this year was done at the direction of the Chinese Government. However, even before this acknowledgment, anyone would be naive to believe that these recent ransomware attacks and cyber attacks are truly perpetuated by rogue criminal organizations within authoritarian China and Russia with no connection to or tacit permission from these authoritarian governments.

So, Ms. Walden, Microsoft Research Asia, MSRA, located in Beijing, notes on their website, "Technologies from MSRA have had a large influence within Microsoft and around the world, and new technologies are constantly born from MSRA. MSRA has achieved breakthrough results in many areas of basic applied computer research, and these results are transferred into Microsoft products.''

Many experts, regulators around the world, have come to, I believe, the rightful conclusion there is no such thing as a private company in China, that virtually everything that

happens in that country happens with at least the -- if not the direction of the Communist Party.

Do you believe that the fact that you are making these products in China makes them more or less vulnerable, more or less -- or makes us more or less vulnerable?

Yes, or -- I mean, are we safer because of that? I don't think so.

*Ms. Walden. Well, thank you for the question. As you pointed out, there are challenges for doing business in China. And we -- right? And we operate on an a zero trust basis, and we operate with our values. We don't --

*Mr. Dunn. They can compel the --

*Ms. Walden. Right.

*Mr. Dunn. -- your information. I mean --

*Ms. Walden. We don't store -- we store no data, no U.S. data, in China. And we operate on the principle of zero trust, and secure that data.

*Mr. Dunn. But the code is also yours, right, and theirs. The codes you write, the software code you write, it is theirs, as well as yours.

*Ms. Walden. For Chinese products and services. But I will tell you this. From an investigation point of view -- and I am in the digital crimes unit -- we go after cyber criminals and their infrastructure wherever they may be, and that will include China, or Russia, or other unfriendly jurisdictions.

*Mr. Dunn. So, I -- we are -- run out of time, but I would say, I just -- like most of us, I think, we are nervous about the fact that you are working so closely with the Chinese Government in China.

I liked your comment on the cryptocurrency, by the way, and it looks more like a security than a currency.

With that I yield --

*Ms. DeGette. The gentleman's time has expired. The chair now recognizes Mr. Tonko for five minutes.

*Mr. Tonko. Thank you, Chair DeGette, and thank you for the hearing.

Our government has an important role in ensuring the nation's cybersecurity, especially related to critical infrastructure. I am sorry to say that high-profile government entities have also been victims of ransomware attacks themselves. In my district alone, the Albany airport, local 911 systems, police departments, and the Albany City Government have all been among those who have been attacked. So, with many government agencies involved, both as targets and as protective actors, I would like to try to get clarity from our witnesses today on just how the government can be better positioned to address this threat, and help respond.

So, Mr. Lee, can you first give us a sense of how it works now?

When a critical infrastructure company is attacked with

ransomware, and they seek assistance from the Federal Government, who do they call? Which agencies get involved?

And most importantly, what services does the government actually provide?

*Mr. Lee. Thank you. I think that the candid answer would be that there is a lot of confusion on who to call, and how to actually organize that. And each government agency is most certainly helpful: CISA, FBI, DoD, so forth. They try to help out. But the expectation on the power company, energy company, and so forth, is that they have to talk to all of them. And there is a lot of confusion on what is actually going to come back as value.

So, while there are good relationships, I think, ultimately, government would do better to be able to communicate with one face, also be able to handle .gov, and the state and local agencies, as well, where there are a lot of cybersecurity issues, and then show the private sector what is working, versus trying to go advocate for services and things to do that they may them not -- they may themselves not be taking full advantage of.

*Mr. Tonko. So who should be that go-to, which face in government?

*Mr. Lee. I don't think most companies really care, but in my opinion it would be CISA. CISA is well established, as a civilian agency, to be the front door to government. That doesn't necessarily mean they are the ones that are going to

do all the work, but to be the coordinator of the interagency process would be much more efficient.

*Mr. Tonko. Thank you.

And Ms. Walden, you spent nearly a decade working on cybersecurity and other national security issues at the Department of Homeland Security. I heard your interaction with a couple of my colleagues on the subcommittee here. But as we consider solutions, are there more services that the government could provide that are currently either in short supply, or not being provided at all?

I heard you encouraging us to provide that full complement, but are there -- those in short supply, or not being done at all?

*Ms. Walden. I think -- and I agree with Mr. Lee here -- that there are services that the government can provide for free, frankly.

I think what is in short supply are the resources, are the workforce, the persons that are able to provide the technical assistance that CISA is authorized to give to private-sector, non-Federal, and Federal entities. There is just a shortage of incident responders, of pen testers, of technical staff that are able to address these issues.

But in terms of authority, legal authority, I think they are -- they exist across the government. I think it is our -- it is the government's job now to really use the full weight of those authorities that they have.

*Mr. Tonko. Thank you. And while it may sound reasonable to have one agency in charge, one concern is that each industry or sector has very specific circumstances and needs. One agency cannot be expected to understand perhaps all the complications of a ransomware attack against a power plant versus a hospital, for example. That is why we have sector-specific agencies to coordinate cyber info sharing with their industry, and act as industry partners. Over the years, however, there have been some challenges about how such agencies coordinate with DHS.

So, Mr. Reiner, what improvements can be made regarding coordination between DHS, sector-specific agencies, and the private sector to address the ransomware threats?

*Mr. Reiner. Mr. Tonko, I think one of the things that we have been most emphatic about, coming out of the Ransomware Task Force effort, is that there may well be -- and I think Charles spoke to this earlier -- there are efforts that are underway that are, actually, pretty phenomenal. There are folks and departments and agencies and companies and individuals that are out there that are fighting this every day, who are actually doing an incredible job. And we really need to commend them. But they need help.

And one of the things that I think that Rob was alluding to is that having an interagency coordinated effort, where you have that one door to turn to when you need that help,

would be immensely helpful. Our argument, coming out of the task force, is that really needs to be coordinated by the White House. The National Security Council really is in a unique position in order to coordinate all elements of national power in a way that, really, nobody else can.

You can look at elements like the NCIJTF. You can look at the JCPO that has just been stood up in DHS. Those may be helpful in this regard, in terms of coordinating interagency assets. But really, at the end of the day, from our assertion, it has got to be out of the White House.

*Mr. Tonko. Thank you very much.

And Mr. Lee, I would ask that you could also respond. I am out of time, but perhaps get word to the subcommittee.

[The information follows:]

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

*Mr. Tonko. Thank you.

*Ms. DeGette. I thank the gentleman. The chair now recognizes Mr. Palmer for five minutes.

*Mr. Palmer. Thank you, Madam Chairman. I want to take this a little different direction.

We have talked a little bit about law enforcement, but on June 14th the heads of state with NATO -- the NATO-allied countries met, and they issued a communique from Brussels, and addressed the issue of the increasingly complex security environment that all these nations are dealing with. And they made this statement -- they issued 79 statements -- number 32, and I will summarize it, that the alliance is determined to deploy the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including those conducted as part of hybrid campaigns, and in accordance with international law.

But they reaffirm a decision as to when a cyber attack would lead to the invocation of article 5, which would be taken by NATO-allied nations on a case-by-case basis, and they said they recognize that the impact of significant, malicious, cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack. That is pretty serious, and I think that is one of the things that we have kind of danced around, we really haven't addressed. We treat all these ransomware attacks as criminal

activity, when they may not be exactly carried out by nation states. But in some cases -- and I think, in particular, Russia and China -- they are at least, if not sanctioned, approved.

And Mr. Lee, I want to direct this to you, because you have military background. We have tremendous capabilities in our military to address this. Does it make sense for us to counterattack, and particularly in some of the nations where the government is really a group of oligarchs with tremendous financial interests?

Just -- could you address that?

*Mr. Lee. Thank you for that question. I think most people in the military would generally like to not get to military force. We want to take all mechanisms available before we get there. And I think there are still plenty left.

However, to directly address the question, I think that we do have to draw certain red lines of what we will and will not accept in this country, and how we are going to respond. And when I have looked at the messaging of NATO and others before on that topic, one of the challenges not only is that we don't specify what that red line is, but we don't tell anybody what we are going to do about it. And so it is not deterrence, it is strategic ambiguity.

*Mr. Palmer. That is --

*Mr. Lee. So if we are going to use military response,

we better well define it.

*Mr. Palmer. Yes, I am not talking about an armed response. I am talking about in the cyber field, because they are attacking infrastructure. And I think our government may have a different definition of what is critical infrastructure than perhaps your organization does, and that is troubling to me. I don't think that we can allow these cumulative attacks to continue, when we know that there -- these groups are giving safe harbor in these nations. There needs to be a price that has to be paid.

I want to transition a little bit away from that and, Ms. Walden, I do appreciate what Microsoft is doing. You have really stepped up, in terms of law enforcement. But I am just not sure that it is enough. And we have had this discussion about whether or not people should pay. And it was mentioned the percentage increase in ransomware attacks, and I just wonder if the fact that people have cyber insurance, and we know that some of these ransomware -- these hackers have hacked into these insurance companies and they know what certain groups are capable of paying, is the insurance helping or hurting?

I mean, when they know that they have the ability to pay, and they negotiate outside of law enforcement, is that helping or hurting?

*Ms. Walden. Well, quite frankly, I don't know if it is helping or hurting. I am not a cyber insurance expert. But

I will say that there is a whole ecosystem out there that supports victims that are attacked by ransom. And cyber insurance companies are just part of that ecosystem. But whether they are helping or hurting, it is the victims that need to make the right business and operational decisions.

*Mr. Palmer. Well --

*Ms. Walden. I would hope that it means to not pay, but I can understand when they do pay.

*Mr. Palmer. Well, one of the things that is missing out on the task force website, and that is whether or not people should pay, and the whole issue of the insurance. That seems to be a pretty substantial omission.

Could you address that, Mr. Reiner?

*Mr. Reiner. Yes, thank you for the question, Mr. Palmer. I think it really, at the end of the day, was the only item that the task force didn't come to a very specific recommendation on, in terms of why. I think there was a general leaning toward, I think, as my colleagues here have noted, making it so that the least amount of money is going to these criminals as possible, and to devise a set of steps so that we could actually move in that direction.

If we were to, for instance, want to prohibit payment now, the ecosystem is simply not ready. It is not prepared for that sort of injunction. So how can we get there?

This -- the report actually does lay out a number of steps, milestones, potentially, that could be taken on over

the course of a couple of years to get us there. That is shoring up the defenses that we are working with that is going after these criminals, so that they don't act with such impunity. There is a good list of steps that need to be taken first, and then maybe we can move in that direction.

*Mr. Palmer. I thank the chair, and I will submit the balance --

*Ms. DeGette. I thank the gentleman.

*Mr. Palmer. -- of my questions in writing.

[The information follows:]

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

*Mr. Palmer. And I yield back.

*Ms. DeGette. I thank the gentleman. The chair now recognizes Mr. Ruiz.

*Mr. Ruiz. Thank you very much, Chair. Today's hearing is focused on ransomware cyber attacks, which are becoming a growing and frequent threat to our businesses, utilities, and government agencies. Ransomware attacks have devastating consequences on their victims. A company or utility being locked out of its networks means lots -- lost of time, lost money, and, in some cases, can also threaten the public's health and safety.

In fact, I have visited Riverside County's Information Technology Center in my district to see what local governments are doing to combat cyber threats, and I have worked with California State University of San Bernardino to strengthen their cyber workforce teaching programs, and for improved pipeline workforce for our nation.

I would like to know more about what happens when a company suddenly finds its employees locked out of their computers due to ransomware, who they can turn to, and what more the government can do to help. So, Mr. Carmakal, I understand you are involved in incidence response at Mandiant. What do companies struggle with the most, or what are their barriers when faced with a ransomware attack?

*Mr. Carmakal. Thank you for the question, sir. So there is a lot of confusion in the early days of an incident.

First of all, people don't actually know what actually occurred. Sometimes you can figure out that you are a victim of a cyber attack, because they see a ransom note that is deployed across all systems. When they see that note, a lot of times those -- the victim organization may call a legal team to help them assess what to do next. They might call an incident response organization to help them investigate the intrusion. They may call their cyber security insurance provider to see whether or not the other third parties that they are engaging can be reimbursed. They may reach out to law enforcement.

But within the first few days there is usually a lot of confusion, and everybody wants to get things back online as quickly as possible. They also want to assess what is the actual true impact of the incident. They want to understand whether or not data was stolen from the environment, and will that information show up on the Internet down the road?

And unfortunately, it is a very complex situation that often takes several days or several weeks to be able to investigate, and to be able to recover the environment. Most organizations that deal with some kind of disruption, best-case scenario, they will be back online within a few days. Realistic scenario, it is going to take them a few weeks, possibly even months, to fully recover every system across the environment. Every situation is different, and there is usually a team of experts that victim organizations call in

and ask for help.

*Mr. Ruiz. Thank you. Thank you.

Mr. Reiner, as we have heard today, one of the most challenging decisions a company faces is whether or not to pay the ransom. In fact, whether or not to prohibit payments of ransom was the one key issue on which your ransomware task force could not reach consensus. So can you please walk us through the considerations here?

And what are the most important recommendations the task force made when it comes to prohibiting ransom payments, and how did you arrive at those priorities?

*Mr. Reiner. Thank you for the question. Yes, it was definitely a contentious discussion around this issue within the task force. And, as we laid down in the report, what we believe is probably the most appropriate way or the most effective way of approaching this is to have a set of steps that need to be taken in order to move in that direction, if that is what is chosen to be done, from a policy perspective.

I think the conclusion of the task force was that, at this point, if you were to mandate the prohibition of payment, that it was just bad policy and that, again, a number of steps really need to be taken in order to move in that direction, one of which is to shore up defenses and get resources to companies and entities, municipalities, what have you, so that they can better defend themselves; take the fight to these ransomware actors in ways that we currently

have not been doing, so they don't get to operate with such impunity; shoring up the cyber insurance market, so that it actually is functioning in response to the level of threats that we are dealing with today.

There is really -- there is a number of steps that we think need to be undertaken, concurrently --

*Mr. Ruiz. Thank you.

*Mr. Reiner. Yes, sir.

*Mr. Ruiz. Dr. Dameff, like you, I am a trained physician, and I know firsthand the heavy reliance hospitals have on digital records and network infrastructure. But people aren't going to stop having medical emergencies, or procedures, or practice medicine when their technology is taken away. What kind of procedures do hospitals need in order to be able to effectively operate during ransomware attack?

For instance, should manual backup procedures exist for when electronic records and machines go down?

How can a hospital practice paper backup for preparedness?

And should those drills be included in accrediting bodies' criteria to be accredited?

*Dr. Dameff. I strongly support the preparation for hospitals to operate under ransomware attack in a manual fashion to the -- to restore those systems as quickly as possible, but not to rely on them to deliver emergent care to

patients that are still going to come in the front door, like you mentioned, still going to come into the emergency department. Whether or not it should be a portion, or a prerequisite, or a condition of hospital accreditation is a complicated one, depending on what level of preparation you are going to require of a particular hospital.

What I can say is that there are current processes in place that are required of every hospital to be prepared for all hazards, things like earthquakes and hurricanes, for which cybersecurity disasters -- truly, these could be disastrous consequences for hospitals -- should be incorporated, and should be prioritized because, generally speaking, cybersecurity attacks -- sorry, cybersecurity and cyber attacks can hit any hospital without geographic predilection or precondition.

What am I trying to say here is that every hospital needs to take this seriously (sic). Every hospital should prepare for taking care of sick patients without the Electronic Health Record and other technical systems. Any preparation efforts for that should be supported, standardized, studied, and spread across the country.

*Mr. Ruiz. Thank you very much.

*Ms. DeGette. I thank the gentleman. The chair now recognizes Mr. Joyce for five minutes.

*Mr. Joyce. Thank you, Chairwoman DeGette, and Ranking Member Griffith for holding today's hearing on the growing

threat of ransomware.

All too often we see our nation's critical infrastructure being attacked from nefarious actors, exposing our vulnerabilities, and ultimately harming our citizens. As a doctor, I am aware of the growing importance of securing patients' personal identifiable information and medical records. This body must take a proactive approach to strengthen all critical infrastructure, and ensure that all Americans' medical data is safe from those who choose to do harm.

Dr. Dameff, let's continue the discussion. In your experience, when a hospital or a health care system is the victim of a ransomware attack, how long are their systems down? Is it days? Is it weeks? Has it gone on for months?

*Dr. Dameff. Great question. We have seen the entire gamut. And it doesn't necessarily always match with how prepared they were; it depends often on who the adversary is, what they particularly deployed.

But one thing I will say is that we need to study this, because, looking at the latest headlines, it seems like cyber attacks are increasing in sophistication, frequency, and, potentially, increasing downtimes. I see more a trend towards weeks to months than I do days, insofar as these devastating attacks are more impactful, and would result in a longer downtime.

*Mr. Joyce. So in this recovery response timeline after

a cyber attack, does the health care system revert to manual patient care systems?

You said something that is somewhat frightening to me. You said you are a generation of doctors who have never used paper charts, or have never written a prescription. As one of the five physicians on this committee here today talking to you, that is frightening to me. How do we respond?

*Dr. Dameff. I think that it is key that we incorporate cybersecurity training and preparation into the next generation of medical education.

*Mr. Joyce. Would that include paper?

*Dr. Dameff. I do. I do think that physicians should be trained to operate in conditions that do not have technology, or to rely on less connected technological backups as a stopgap measure for patient care.

*Mr. Joyce. When talking about ways to prevent or mitigate the effects of a cyber attack on health care systems, some individuals talk about the cloud, or having a system backed up. Are these ultimately foolproof ways to ensure that a hospital system or a health care provider does not have to pay the ransom, or the ransomware attack, or that patients are less impacted?

*Dr. Dameff. I think that this trend towards centralization of medical device management, for example, or Electronic Health Records into the cloud is a trend we are not going to see change.

I would defer to the specific security protections offered by such cloud architecture to other members of the panel, as it is not my expertise. But I will say that it is a two-edged sword, if you will. The centralization of these into the cloud mean that a single attack on a cloud provider offering services to many hospitals across the country, if attacked, could impact all of them at once.

So that being said, many hospitals are not well equipped to defend their systems, as it is. So do you offer increased protections from the cloud, more so than you would at individual hospitals, taking the risk that, if that particular cloud provider went down, you know, hundreds of hospitals could be hit?

This is something we are going to have to figure out, and, quite frankly, we do not have the data to make that decision, currently.

*Mr. Joyce. Dr. Dameff, I would be remiss if I did not reach out and thank emergency physicians, emergency nurses, emergency technicians as we have faced a pandemic, and as you continue to face the ransomware attacks that are occurring in the medical community. As someone who previously worked at Johns Hopkins Bayview Emergency Department, I have great respect for the work that you continue in the face of this pandemic, and I think I acknowledge that today and thank you.

Madam Chair, I remain -- I yield my remaining few seconds.

*Ms. DeGette. Thank you, Mr. Joyce. And I think that the entire panel and the entire Congress would echo your sentiments, thanking --

*Mr. Joyce. Thank you, Chair DeGette.

*Ms. DeGette. -- emergency room personnel. Thank you.

The chair now is pleased to recognize Mr. Peters for five minutes.

*Mr. Peters. Thank you, Madam Chair. Thanks to the witnesses for being here.

Dr. Dameff, you have got all the questions, but you are from San Diego, so I just have to ask you a couple.

First of all, thanks for your great work.

And just down the street from you, a major hospital system suffered this very attack, and I assume will -- as they ease out of that, or as they climb out of that, we will learn more about what protocols could be.

I have heard you talk about making sure that, in the aftermath of an attack, that hospitals are prepared to operate without their technology; also, to define protocols that hospitals might be able to rely on to prepare to defend themselves against these hacks.

One question I just haven't had -- you haven't -- heard you answer, and forgive me if I missed it, but should we be disconnected a little bit more?

I have often wondered if there is a way to take a unit like a hospital, and to have some sort of way to fence it off

so that they can operate internally in a connected way without being so exposed. And that may be a question for you, or for some of the people on the panel, but I am curious about that.

*Dr. Dameff. I do believe we should invest in technology that limits the exposure of hospitals. Traditionally speaking, as I mentioned previously, hospitals are soft targets. They generally have flat networks, meaning that they are often employing the best practices for network segmentation. And as a consequence, they are more at risk for rapid spread of ransomware, for example.

So this concept of isolating critical sections of the hospital, and being able to rely on those systems without risk of ransomware would require a lot of those technological solutions. They are costly and, as mentioned previously, there are a lot of health care systems that will not have the ability to deploy such technology without resources and additional guidance.

And so, for that, I would encourage that type of isolation. But I fear we are not going to get to it. Instead, I think we are, unfortunately, going to have to rely on just preparing for an inevitable attack, and limiting the damage to patient care while we wait for system restoration.

*Mr. Peters. And also deploying defined protocols or best practices, I guess, as it would be -- maybe we could help define.

You know, I appreciate that. And I also wanted to follow up on comments from questions from the chair and from Ms. Schakowsky about what the duty is of private organizations to take care of their stuff.

You know, I thought a lot about Equifax -- not to pick on any particular company -- but there is a company that is performing a public function with a lot of private data. And it seemed to me that the loss of that data to the malefactors really didn't hit their bottom line. And so I have often wondered if the companies that do this kind of work, sort of like, in a way, providing a public service, are appropriately incentivized to take care of that data.

Maybe, Ms. Walden, I would direct this to you. Your testimony said that we should make sure that companies make it harder to get in, limit the scope of damage, and prepare for the worst. I guess -- do you believe that companies are appropriately -- to incentivize on -- from the bottom line to take care of individuals' data, or is that something that the government has to define better?

*Ms. Walden. First, as a victim of the OPM breach years ago --

*Mr. Peters. OPM, and the DNC, but I changed my cell phone number. That is a different situation --

*Ms. Walden. Those are different situations. But I do think that companies need to be held to a standard to protect private data. But these cyber attacks are more than just

about data leakage, right? They are interrupting business operations.

*Mr. Peters. Right.

*Ms. Walden. And I do think that there is a role for the private sector in making sure that they prevent these criminal actors from getting into their systems in the first place. There are some very simple things that can take place that we described here: multifactor authentication, patching your software, et cetera.

But all that is to say is -- I think we need to raise the collective security of critical infrastructure owners and operators, and we -- we need to put the onus on both the government, to protect the critical infrastructure, and the private sector that owns and operates the critical infrastructure --

*Mr. Peters. Don't get me wrong. I actually, really, am a believer that the private sector has the -- is the appropriate place for these solutions to be investigated and developed. What I don't -- what I am -- just to make sure that I am clear, is that I am not sure that companies are incentivized in a way that would make them deploy the best practices.

So, even if we knew what those best practices were, even if we defined them from sector to sector, what is going to make the next company who has got private information invest in that, knowing that maybe the loss of that information

doesn't directly affect their bottom line?

*Ms. Walden. I would agree. I think many companies aren't properly incentivized to protect their data.

*Mr. Peters. I am out of my -- I am out of time. I would just suggest that we might want to think about defining a duty of care in a piece of legislation that would just make sure that everyone is properly noticed that they have to do the right thing.

And Madam Chair, with that I yield back.

*Ms. DeGette. I thank the gentleman. The chair now recognizes Ms. Schrier for five minutes.

*Ms. Schrier. Thank you, Madam Chair, and thank you to our witnesses.

When we hear the term "ransomware,'' we often think of high-dollar ransoms and large companies. But as all of you pointed out, individuals and communities are also affected by these attacks when they can't get gas to go to work, when their school or local hospital is impacted by an attack, or when their own data is compromised.

I have heard from local hospitals about the immense cost and manpower it takes to try to harden a whole system to prevent a cyber attack; with my hospital, who is training up a workforce to not fall prey to phishing; and then to recruit and hire the best and brightest in cybersecurity, as you mentioned.

Dr. Dameff, I can tell you, from common experience, that

just a few hours of power outage completely handicapped my ability to take care of patients, so I can only imagine how this sort of thing would impact a hospital, especially for days on end. And you already described for my colleague, Mr. Griffith, how those impacts on patient care may be felt more acutely in lesser-resourced and rural hospitals. Could you be a little bit more specific about how sister hospitals, if there even are sister hospitals, local entities, private-sector actors, and the Federal Government could better support specifically those health care systems, so that they have the resources they need?

*Dr. Dameff. Thank you so much for that question.

I think the first and most important thing is the preparatory efforts to prevent and then mitigate the impacts of those attacks. So, looking at your particular geographic area, and understanding where are the lynch pin hospitals, right? Which ones are providing trauma services? Which ones are stroke centers?

These types of specialized hospitals, who take care of hyper acute patient care, should be identified early, and prioritized for that type of preparation, as well as resources to ensure that, when they do go down, or when they are attacked, they are able to fail gracefully as much as possible, while still taking care of patients. So there is a preparatory step in that.

Second, in the response phase of this, I think it is

common for a hospital to reach out to law enforcement early. I think that has been a pretty common theme, in that they will reach out to the FBI to help with investigatory efforts and response. But whether or not that type of communication transcends to other government agencies such as CISA or the FDA, even if medical devices are involved, can sometimes be -- not happen.

And so I think that is partly the responsibility of a particular hospital, but also of the bodies that accredit hospitals, as well as local public health authorities in being able to quickly propagate meaningful metrics of patient care to authorities that can help, who can bring resources in the hour of need to help hospitals still take care of patients while addressing that.

*Ms. Schrier. That is --

*Dr. Dameff. So that type of interagency communication is lacking.

*Ms. Schrier. That is really helpful. And I know, in Washington State, our Washington State Hospital Association does these kinds of drills with hospitals to help them prepare.

And then, speaking of incentives, I know a hospital's reputation is really integral to its ability to serve the public. It seems like one of the things we need to communicate to the public is that, even with the best preparation, these attacks are so common that you can still

be hit. Do you think that is a role for public -- you know, for the government, for the private sector, to kind of communicate this to the public?

*Dr. Dameff. The communication -- oh, thank you very much -- the communication of that is rather difficult.

I have always said that there should be no competitive advantage in health care cybersecurity. Right? There should never be billboards saying, "Come to our hospital, we didn't have this happen,'' because, quite frankly, I would agree with you that, because of increased -- the sophistication of these types of attacks, no one is immune from this. No health care organization is immune, regardless of their cybersecurity budget.

So at the end of the day, I think communicating that it is a unfortunate consequence of the hyperconnectivity of health care, that there are steps being done and resources provided to hospitals to prepare and mitigate that is key, while still trying to restore trust in consumers and how they approach a particular hospital for health care.

*Ms. Schrier. Thank you.

*Dr. Dameff. That is key. That is really important.

*Ms. Schrier. I have one last question for Mr. Reiner.

Now, I appreciate your comments about our country not really being quite at the right place to be able to prohibit payment of ransoms, even though that might slow or stop these cyber attacks. So, for now, what can companies do, for

example, to have duplicate systems, a wall between them so that they could recover afterwards, maybe without paying the ransom?

*Mr. Reiner. So one of the pieces that we haven't really discussed here today, outside of some of the elements of what companies can be doing to prepare, is to actually -- what we discovered through our process is that a lot of companies actually don't have a plan. They actually haven't vetted out, at the executive level, what to do, whether or not to pay. And they have companies that they can turn to that can help them through that process, whether it is their insurance company, or a forensics company, or some of the folks on the panel here with me today.

But actually having that in place ahead of time, companies do tabletop this. They do exercise against it, but not all of them. And I think that is a resource that everyone should have in hand, to have a checklist, to have an actual plan to help make you make that decision if you do get hit.

*Ms. Schrier. Thank you very much. I yield back.

*Ms. DeGette. I thank the gentlelady. The chair now recognizes Mrs. Trahan for five minutes.

*Mrs. Trahan. Well, thank you, Chairwoman DeGette, for this important, certainly informative, and timely hearing.

The threat that hackers pose to businesses and institutions is so real, and the increasing frequency and

severity of the attacks is deeply disturbing. You know, like so many of my colleagues and the panelists testifying today, I am concerned that cyber attacks are becoming especially common place within critical public service sectors, ranging from health care to education. In fact, a public university in my district was recently hit by a cyber attack that shut down operations for a week.

Ransomware has become one of the most attractive tools for criminals because of how lucrative it can be, often without much effort. And hackers find vulnerable caches of critical data being stored by organizations like hospitals, schools, and sometimes even local governments, and then use ransomware to effectively lock the organization out of their own data until they agree to pay up.

Now, what has become clear is that improving our cyber defenses is not enough to combat this threat. We need to, you know, find ways to disrupt the ability of criminals to demand and receive ransom payments without consequence.

The Internet has allowed for ransoms to be paid remotely through digital gift cards and, of course, cryptocurrency such as Bitcoin. So, Ms. Walden, could you just explain what it is about cryptocurrencies that make them the chosen method of payment for ransoms in this type of cyber crime?

*Ms. Walden. Yes, and thank you for that question.

So cryptocurrency, the technology underlying cryptocurrency, blockchain technology, allows for a

transparent payment system that is decentralized and distributed, and it allows for, at the same time, pseudo-anonymity. It is a complicated word to say for me, but that essentially means that, while you can track the transaction, and you can see exactly, you know, the hops of money from one wallet to another, the on-ramps and the off-ramps, you can't necessarily see the persons behind the transaction. You can't see the person that owns the wallet.

So that is one thing that makes it attractive. The other is that the transactional costs in the crypto economy are much lower than in the traditional fiat economy. So central banking systems are just more expensive.

*Mrs. Trahan. Sure.

*Ms. Walden. And then, finally, the third thing is that it is difficult to trace. Not impossible, but it is difficult to trace. So -- but it is -- and it is borderless. So you can have money move quickly and effectively across borders. There is no central banking authority that sort of maps it out. And the use of Bitcoin, in particular, is prevalent because it is the most widely used currency, virtual currency. It is easy to get, it is liquid --

*Mrs. Trahan. Yes.

*Ms. Walden. And victims can -- can easily put that into the system.

*Mrs. Trahan. Yes. And you --

*Ms. Walden. I hope that answered your question.

*Mrs. Trahan. Yes, it definitely did, and it is great to have that thorough answer on the record, because an oft-cited rationale for the use of cryptocurrency is the lack of visibility into parties conducting transactions, and a lack of clarity regarding government relations.

And so, Mr. Reiner, I am wondering, you know, if you could answer this question. You know, cryptocurrency exchanges operate in the United States. They are subject to certain regulations. But clearly, there are opportunities to expand the applicability and/or enforcement of those regulations. And if so, if you agree with that statement, you know, what specifically do you recommend?

*Mr. Reiner. I would agree with that, and thank you for the question.

I think the task force, as it came together, recommended a number of steps that could be taken to -- and I think it is important to note here that the task force's position on this wasn't necessarily that cryptocurrency is the problem, right? Cryptocurrency is something that I think can add value to -- in a number of different ways, but that, in this instance, it is something that is being abused.

There are a number of steps that could be taken to pull elements of the cryptocurrency ecosystem into existing regulatory regimes, whether that is expanding the application of know-your-customer rules, the anti-money laundering rules that are already available.

I think, to your -- to the nature of your question, though, something that is incredibly important here is some of this is outside of U.S. jurisdiction, and so there -- and we need to be working very closely with international partners so that they can be taking these steps with actors in their spaces to do the same thing.

I think a number of the actors that we engaged with through the Ransomware Task Force process made it very clear that that is a conversation they want to be a part of, to positively contribute in that direction. I think there is real opportunity there.

*Mrs. Trahan. Great. Well, thank you. I am out of time. I will submit the rest of my questions for the record.

[The information follows:]

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

*Mrs. Trahan. Thank you, Madam Chair.

*Ms. DeGette. I thank the gentlelady. The chair now recognizes Mr. O'Halleran for five minutes.

*Mr. O'Halleran. Thank you, Madam Chair and the ranking member, for today's hearing.

You know, securing the infrastructure for America is critical. We are all in agreement with that. I haven't seen anything today that would tell me that we aren't. Issues like Colonial Pipeline, how many more times do we have to see this occur, and not get serious about this? Year after year after year, something comes up, where this becomes an issue. And now it is a critical issue, in my mind, for -- and I know the doctors' minds -- for the health and welfare of the people of America.

Big companies have tons of cyberspace security, and even they are attacked frequently. Should we hope and pray that we won't be targeted, or should we do something about this?

In Arizona we are facing record heat and droughts every year. I am concerned what would happen to vulnerable populations, especially older Americans, if our power, water utilities, and others went down. Our families could be left without running water or power for days, weeks, who knows, as new developments and technologies occur. I hope we can learn from today that this has to be a priority for our businesses in America and our government.

Ms. Walden, I am sure you agree that we need to do more

to disrupt ransomware. You said in your testimony that Microsoft is working to make ransomware less profitable and more difficult to employ. What does that mean? What are you doing?

*Ms. Walden. Thank you for the question. As you aptly pointed out, there is an imbalance, right, that allows ransomware to proliferate: one, it is a highly profitable crime; second, there is -- there are few barriers to entry. I could get into the crime of ransomware, and I haven't coded since 1985. So it is just off balance.

And so our opportunity at Microsoft is to disrupt its scale. And what does that mean? That means that we go after the infrastructure. So we go after payment systems that support the profitability, and we disrupt that. But we also make it harder for our products and services to be used to proliferate ransomware. And we make the entry of the criminal to -- more difficult, right?

So that means tearing down payment systems where we can, or the ability for ransomware actors to receive payment. And that means tearing down negotiation opportunities between the ransomware criminal gang and the victim. That means disrupting their ability to easily commit this crime. And that also means, from a threat actor perspective, working closely with our law enforcement partners to bring justice to these criminals that propagate the crime.

*Mr. O'Halleran. Thank you very much for that answer.

Mr. Carmakal, what type of information sharing is there between private sector and the U.S. Government when it comes to attacks on businesses?

And how do we recommend -- or you recommend -- we can improve this?

It is obvious from today that there is a lot of areas where information sharing does not go on. And I don't know how this whole system works if we don't share that information. Mr. Carmakal, please.

*Mr. Carmakal. Yeah, thank you, sir. I think there is an opportunity for us to do a better job of sharing information between victim organizations and the rest of the world. But they need to do it in a way where they don't feel like they are going to be penalized for having a data security incident.

There is a common trend of victims becoming a second victim because of public shaming by other organizations, by the general public when there is a cybersecurity incident. So we need to create an opportunity and facilitate a way for victim organizations to be able to share information about active attacks, about compromises with some central governing body or some agency that is able to disseminate that information in a quick and actionable way.

A lot of times, when we see threat actors operate, they conduct intrusions at dozens of organizations at the same time. And if we are able to take information from one victim

organization and share it with the community, it helps us disrupt threat actors, helps us increase the cost of threat actor operations, and I think that is one of the many ways in which we could all take collective actions to curb this problem.

*Mr. O'Halleran. I thank you.

And Madam Chair, I just don't believe that we are going to get the type of process moving forward that we truly need, as a nation, without clearly identifying how we are going to communicate with one another in this area, whatever privacy laws have to be placed, or whatever has to be done to allow people to be able to talk to one another.

So with that, I yield.

*Ms. DeGette. Thank you. I thank the gentleman.

The committee has a storied tradition of allowing members of the full committee to question. And that is particularly useful today because we have our resident technology expert with us, Mr. McNerney. So I am pleased to recognize him for five minutes.

*Mr. McNerney. Well, I thank the chair for the hearing, and the witnesses for your testimony. I thank the chair and the ranking member for allowing me to waive on this morning -- or this afternoon, now.

Cybersecurity defenses are primarily intended to safeguard organizations' IT systems, but many critical sectors are relying on OT systems such as SCADA systems and

PLCs to operate machinery or industrial controls.

OT system attacks are increasing in severity and frequency. For instance, the case of Colonial Pipeline attack, the company proactively shut down its OT systems in response to ransomware attacks on its IT system. Mr. Lee, how serious and widespread is the ransomware threat on OT systems?

*Mr. Lee. Thank you for that question. It is significantly more frequent than people would realize. There is, you know, some weeks that we go where we might have five different incident response cases on just OT systems that never go public.

And so I think, you know, I agree with a lot of the recommendations around removing the stigma around this. But also, we have to make sure that there is value back to those organizations. So there is a lot of desire of you must communicate to the government. But if there is no value back to those organizations in doing that, it is just not a top priority.

*Mr. McNerney. Well, is there any government support for companies in dealing with live OT threats?

*Mr. Lee. I think that, while there are many great members in the government, and there is some expertise there, I would say that the OT cybersecurity expertise is very much more in the private sector than in government, and it is very nascent in the government to be able to handle that.

I would say, from a policy position, we should probably more proactively partner with those folks doing that work, and make sure that we remove those barriers to get things like visibility in those systems. I think it was mentioned previously that you almost benefit when you have ransomware by the fact that you know it. There is a lot of these cases that people just simply don't know that they are getting compromised.

*Mr. McNerney. Thank you.

Mr. Carmakal, over the years in your career you have helped organizations across the globe respond to some of the most catastrophic cybersecurity attacks and insurance instances. Based on your experience, what risks will ransomware attacks on OT systems pose?

And how can the potential victim organizations best protect themselves?

*Mr. Carmakal. Yeah, and thank you for the question, sir. Ransomware attacks against operational technology systems have the potential to be incredibly devastating. We had the potential to see true kinetic responses and impacts that everyday people may be able to observe. And so there is certainly a risk and a threat there.

Generally speaking, a lot of organizations, they struggle to think about security, from an operational technology perspective. Part of that challenge is with governance. A lot of times the person that is responsible

for cybersecurity doesn't always have the governance and authority to be able to apply cybersecurity protocols and policies on operational technology environments. A lot of times it is the business owner or the asset owner that is responsible for cybersecurity. And a lot of times those asset owners don't actually have cybersecurity experience. And so there is some fundamental challenges that are out there.

I think we need to continue to focus on operational technology security. There is a lot of potential real-world impact that can occur there. And I think it is a natural evolution of the threat that we are seeing today.

*Mr. McNerney. Thank you.

And Mr. Lee, what role can the public-private partnerships that the Administration announced in April play in shoring up some of these vulnerabilities in OT systems?

*Mr. Lee. Yeah, the very first thing is partnership with the sector, but more specifically in actually understanding what the sectors need.

A great example, there was many things recommended here today about patching and phishing, you know, training and similar, that are absolutely appropriate in the enterprise. And they would make a top-10 list in operations technology security. There is a lot of enterprise security people that come into operations environments thinking that the playbook that they run in IT is what they should do in OT. And there

have been more power outages in the United States to people patching systems than Russia, China, and Iran, combined.

So when we look at OT, we need to make sure that the government partners understand: How do you operate a gas plant different than a nuclear power plant; What do you need to see in these standards, other than just what we think best practices are from a higher level?

*Mr. McNerney. Thank you.

Mr. Reiner, thank you for the recommendations from the IST. The discussion today has been entirely focused on attacks on institutions. I am a little curious about attacks on individuals. Are those attacks continuing to escalate, as they are (sic)?

Is there any resource in the government for people that need help in that situation?

Mr. Reiner, you want to answer that?

*Mr. Reiner. I think the preponderance of -- I mean, this is a profit-driven enterprise, and so the attackers are looking for those -- they do their research, they do their analysis to find those that are not only the most vulnerable, but are going to be the most lucrative. And I don't really think that they necessarily discriminate, per se.

I personally am not as familiar with attacks that are targeted against individuals, as much as they are against organizations, which has the large attack surface that can be taken advantage of, et cetera, and that has the resources,

actually, to pay these ransoms that these criminals are really looking for.

*Mr. McNerney. Okay, thank you. I yield back.

*Ms. DeGette. I thank the gentleman, and I really want to thank again all of our witnesses for participating in today's hearing. It was a really excellent -- both the ranking member and I agreed, it was an excellent panel, gave us a lot of good information. And we will be following up with all of you on your recommendations.

I want to remind members that, pursuant to committee rules, they have 10 business days to submit their additional questions for the record to be answered by the witnesses who have appeared. And I would ask the witnesses to please agree to respond promptly to any of those questions that you might receive, because they will be very helpful to us in developing further legislation and approaches.

[The information follows:]

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

*Ms. DeGette. Also, the ranking member and I would like to insert into the record by unanimous consent a report on cybersecurity by the ENC Republican staff dated December 7, 2018.

And without objection, it is ordered.

[The information follows:]

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

*Ms. DeGette. And with that, the subcommittee is adjourned.

[Whereupon, at 1:11 p.m., the subcommittee was adjourned.]