RESPONDING TO RANSOMWARE: EXPLORING POLICY SOLUTIONS TO A CYBERSECURITY CRISIS

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

MAY 5, 2021

Serial No. 117–12

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

44–930 PDF WASHINGTON : 2021

COMMITTEE ON HOMELAND SECURITY

BENNIE G. THOMPSON, Mississippi, *Chairman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
DONALD M. PAYNE, JR., New Jersey
J. LUIS CORREA, California
ELISSA SLOTKIN, Michigan
EMANUEL CLEAVER, Missouri
AL GREEN, Texas
YVETTE D. CLARKE, New York
ERIC SWALWELL, California
DINA TITUS, Nevada
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
VAL BUTLER DEMINGS, Florida
NANETTE DIAZ BARRAGÁN, California
JOSH GOTTHEIMER, New Jersey
ELAINE G. LURIA, Virginia
TOM MALINOWSKI, New Jersey
RITCHIE TORRES, New York
JOHN KATKO, New York
MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
JEFFERSON VAN DREW, New Jersey
RALPH NORMAN, South Carolina
MARIANNETTE MILLER-MEEKS, Iowa
DIANA HARSHBARGER, Tennessee
ANDREW S. CLYDE, Georgia
CARLOS A. GIMENEZ, Florida
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
KAT CAMMACK, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York

HOPE GOINS, *Staff Director*
DANIEL KROESE, *Minority Staff Director*
NATALIE NIXON, *Clerk*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

YVETTE D. CLARKE, New York, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
ELISSA SLOTKIN, Michigan
KATHLEEN M. RICE, New York
RITCHIE TORRES, New York
BENNIE G. THOMPSON, Mississippi *(ex officio)*
ANDREW R. GARBARINO, New York, *Ranking Member*
RALPH NORMAN, South Carolina
DIANA HARSHBARGER, Tennessee
ANDREW CLYDE, Georgia
JAKE LATURNER, Kansas
JOHN KATKO, New York *(ex officio)*

MOIRA BERGIN, *Subcommittee Staff Director*
AUSTIN AGRELLA, *Minority Subcommittee Staff Director*
MARIAH HARDING, *Subcommittee Clerk*

CONTENTS

RESPONDING TO RANSOMWARE: EXPLORING POLICY SOLUTIONS TO A CYBERSECURITY CRISIS

Wednesday, May 5, 2021

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND INNOVATION,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:30 p.m., via Webex, Hon. Yvette Clarke [Chairwoman of the Subcommittee] presiding.

Present: Representatives Clarke, Jackson Lee, Langevin, Rice, Torres, Garbarino, Norman, Harshbarger, and Clyde.

Also present: Representative Katko.

Chairwoman CLARKE. The Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation will come to order. Without objection, the Chair is authorized to declare the subcommittee—oops, excuse me. Let me move forward.

Good afternoon and thank you to our witnesses for joining us today to discuss how we can respond to the ransomware crisis.

You know, I first chaired this subcommittee over 10 years ago. While ransomware is not a new problem, the number of cases and the financial impact has skyrocketed since then. That is why I wanted to focus on ransomware at our first subcommittee hearing this year. We must understand the problem we are facing, learn more about how the Federal Government should respond, and do something.

Estimates show that ransomware victims paid $350 million in ransom payments last year. Among those victims were 2,400 U.S.-based governments, health care facilities, and schools. As the COVID–19 pandemic forced governments and businesses to shift to remote work, thousands found themselves locked out of their networks as cyber criminals demanded ransom payments. These attacks are more than a mere inconvenience. They are a National security threat. It is time for bold action rooted in robust partnerships between the Federal Government and its State, local, and private-sector partners.

In the coming days, I will introduce the State and Local Cybersecurity Improvement Act, which will authorize $500 million in annual grants to State, local, territorial, and Tribal governments to strengthen their cybersecurity. As the ever-increasing number of

ransomware attacks on State and local governments demonstrates, adequate treatment in cybersecurity has been lacking and more resources are needed.

Just last week we saw some ransomware attacks that released sensitive law enforcement information from police departments in Washington, DC, and Presque Isle, Maine, showing that cities, large and small, are vulnerable to this type of cyber crime. This legislation would ensure funding is available while insisting State and local governments step up to prioritize cybersecurity in their own budgets.

I am proud of the bipartisan support this bill has received on this committee and look forward to working with Ranking Member Garbarino along with Chairman Thompson and Ranking Member Katko to get this critical bill enacted. I hope this hearing will give us an opportunity to learn more about the challenges State chief information officers face under current funding constraints and how they would be able to use additional resources to strengthen their defenses to ransomware.

While State and local governments are some of the most notable victims of ransomware, this crisis affects many private businesses in the United States and around the world. Combatting this threat will require coordination between the public and private sectors and all levels of government.

The Ransomware Task Force report released last week provided 48 recommendations on what Government and industry can do to address this crisis in the coming months and years. I am excited to have 2 of those co-chairs of the task force here today to share more information on the recommendations.

As Secretary Mayorkas has made clear in announcing that addressing ransomware would be the first of DHS's 60-day sprint on pressing cybersecurity challenges, responding to ransomware is a priority for his administration. It is definitely a priority for this committee and many in Congress.

So, I hope that this hearing will help further the conversation on how the private sector, Congress, the Executive branch, and State and local governments can collaborate to address this crisis head-on. In particular, I am interested to learn how other committee priorities, including developing a cyber incident reporting framework, could improve our understanding of ransomware trends and how to defend against such attacks.

Relatedly, I am interested to hear how CISA can play an important role in information sharing and coordinating this response. As the agency that works closely with governments at all levels and the private sector on cybersecurity matters, I know it will have a significant role on this issue going forward.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

MAY 5, 2021

Good afternoon and thank you to our witnesses for joining us today to discuss how we can respond to the ransomware crisis.

I first chaired this subcommittee over 10 years ago. While ransomware is not a new problem, the number of cases and the financial impact has skyrocketed since then. That's why I wanted to focus on ransomware at our first subcommittee hear-

ing of the year. We must understand the problem we're facing and learn more about how the Federal Government should respond.

Estimates show that ransomware victims paid $350 million in ransom payments last year. Among those victims were 2,400 U.S.-based governments, health care facilities, and schools. As the COVID–19 pandemic forced governments and businesses to shift to remote work, thousands found themselves locked out of their networks as cyber criminals demanded ransom payments. These attacks are more than a mere inconvenience—they are a National security threat. It is time for bold action rooted in robust partnerships between the Federal Government and its State, local, and private-sector partners.

In the coming days, I will introduce the State and Local Cybersecurity Improvement Act, which would authorize $500 million in annual grants to State, local, territorial, and Tribal governments to strengthen their cybersecurity. As the ever-increasing number of ransomware attacks on State and local governments demonstrates, adequate investment in cybersecurity has been lacking, and more resources are needed. Just last week, we saw ransomware attacks that released sensitive law enforcement information from police departments in Washington, DC and Presque Isle, Maine, showing that cities large and small are vulnerable to this kind of cyber crime.

This legislation would ensure funding is available, while insisting State and local governments step up to prioritize cybersecurity in their own budgets. I am proud of the bipartisan support this bill has received on this committee and look forward to working with Ranking Member Garbarino, along with Chairman Thompson and Ranking Member Katko, to get this critical bill enacted. I hope this hearing will give us an opportunity to learn more about the challenges State chief information officers face under current funding constraints and how they would be able to use additional resources to strengthen their defenses to ransomware.

While State and local governments are some of the most notable victims of ransomware, this crisis affects many private businesses in the United States and around the world. Combatting this threat will require coordination between the public and private sector and all levels of government. The Ransomware Task Force Report released last week provided 48 recommendations on what Government and industry can do to address this crisis in the coming months and years. I am excited to have 2 of the co-chairs of the Task Force here today to share more information on the recommendations.

As Secretary Mayorkas has made clear in announcing that addressing ransomware would be the first of DHS's 60-day sprints on pressing cybersecurity challenges, responding to ransomware is a priority for this administration. And it is definitely a priority for this committee and many in Congress. So, I hope that this hearing will help further the conversation on how the private sector, Congress, the Executive branch, and State and local governments can collaborate to address this crisis. In particular, I am interested to learn how other committee priorities—including developing a cyber incident reporting framework—could improve our understanding of ransomware trends and how to defend against such attacks. Relatedly, I am interested to hear how CISA can play an important role in information sharing and coordinating this response. As the agency that works closely with governments at all levels and the private sector on cybersecurity matters, I know it will have a significant role on this issue going forward.

With that, I would like to again thank the witnesses for being here.

Chairwoman CLARKE. With that, I would like to again thank the witnesses for being here. The Chair now recognizes the Ranking Member of the subcommittee, Mr. Garbarino from New York, for an opening statement.

Mr. GARBARINO. Thank you, Chairwoman. Thank you very much. Thank you to the witnesses for being here today. This is a very important issue.

The global cost of ransomware has risen to $20 billion a year. Over the past several years ransomware attacks have increased at an alarming rate. Attacks like NotPetya and WannaCry have had devastating impacts to critical sectors across the globe. Just a few months ago, both the Bay Shore and Lindenhurst School Districts on Long Island in my district were hit with cyber attacks.

I am determined to work with hospitals, schools, and small businesses in New York's Second District and across the country to im-

prove their cybersecurity posture in the wake of increasing threats. I believe it now more important than ever to work with agencies like CISA, the Secret Service, and the Treasury Department to combat malicious cyber actors from targeting our struggling small businesses, health care institutions, and State and local governments. We must think of new, innovative ways to interrupt cyber criminals' ability to see this as a financially viable way of doing business.

It should come as a surprise to no one in this hearing that these ransomware attacks have devastating real-world consequences for Americans. Every minute that a hospital goes down is a minute of missed critical care. The same goes for almost every industry. We must work to put a stop to this. We need to double down on ensuring State and local entities and small businesses are prepared and adopt basic cybersecurity best practices to mitigate cyber risks. These practices can include two-factor authentication, strong passwords, retaining backups, developing a response plan, and updating software.

CISA, in partnership with the Multi-State Information Sharing and Analysis Center, also covers several no-cost services across the Nation that should be leveraged by State and locals and the private sector. This includes the Joint Ransomware Guide developed both by CISA and the MS–ISAC that includes industry best practices and serves as consolidated resources for SLTT and the private sector.

I am a proud original cosponsor of the Chairwoman's State and Local Cybersecurity Improvement Act. While we all can agree more resources for our State and local governments are necessary, we must also ensure these funds are spent responsibly and effectuate meaningful impacts on risk reduction.

This important bill is a tremendous step forward in our fight, but we cannot stop there. While somewhere near only 2 percent of all cryptocurrency payments are nefarious, we know that most, if not all, ransomware payments utilize the anonymity of cryptocurrencies. We must adopt an all-of-the-above approach to dealing with this scourge. There is no single silver bullet.

I look forward to hearing from our witnesses today about the innovative solutions Congress should consider as we work to degrade and ultimately eliminate the viability of ransomware.

Thank you, Madam Chairwoman, for bringing this important issue before us today. I yield back.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW R. GARBARINO

The global cost of ransomware has risen to $20 billion a year.

Over the past several years ransomware attacks have increased at an alarming rate. Attacks like NotPetya and WannaCry have had devastating impacts to critical sectors across the globe.

Just a few months ago, both the Bay Shore and Lindenhurst school districts on Long Island were hit with cyber attacks. I am determined to work with hospitals, schools, and small businesses in New York's 2d district and across the country to improve their cybersecurity posture in the wake of increasing threats.

I believe it is now more important than ever to work with agencies like CISA, the Secret Service, and the Treasury Department to combat malicious cyber actors from targeting our struggling small businesses, health care institutions, and State and local governments.

We must think of new innovative ways to interrupt cyber criminals' ability to see this as financially viable way of doing business.

It should come as a surprise to no one in this hearing that these ransomware attacks have devastating real-world consequences for Americans. Every minute that a hospital goes down is a minute of missed critical care. The same goes for almost every industry.

We must work to put a stop to this.

We need to double down on ensuring State and local entities and small businesses are prepared and adopt basic cybersecurity best practices to mitigate cyber risks. These practices can include: Two-factor authentication, strong passwords, retaining backups, developing a response plan, and updating software.

CISA, in partnership with the Multi-State Information Sharing and Analysis Center (MS–ISAC), also offers several no-cost services across the Nation that should be leveraged by State and locals and the private sector. This includes the Joint Ransomware Guide, developed by both CISA and the MS–ISAC that includes industry best practices and serves as a consolidated resource for SLTT and the private sector.

I am a proud original cosponsor of the Chairwoman's State and Local Cybersecurity Improvement Act. While we all can agree more resources for our State and local governments are necessary, we must also ensure these funds are spent responsibly, and effectuate meaningful impacts on risk reduction. This important bill is a tremendous step forward in our fight, but we can't stop there.

While somewhere near only 2 percent of all cryptocurrency payments are nefarious, we know that most, if not all ransomware payments utilize the anonymity of cryptocurrencies.

We must adopt an "all of the above" approach to dealing with this scourge. There is no single silver bullet.

I look forward to hearing from our witnesses today about the innovative solutions Congress should consider as we work to degrade, and ultimately eliminate the viability of ransomware.

Thank you, Madam Chair, for bringing this important issue before us today.

Chairwoman CLARKE. I thank the Ranking Member. Members are also reminded that the committees will operate according to the guideline laid out by the Chairman and Ranking Member in their February 3 colloquy regarding remote procedures.

The Chair now recognizes the Ranking Member of the full committee, the gentlemen from New York, another gentleman from New York, Mr. Katko, for an opening statement.

Mr. KATKO. Thank you, Chairwoman, from the great State of New York. I appreciate it. Ranking Member Garbarino, thank you for holding this important hearing.

Mr. Krebs, it is always good to see you. It has been 24 hours since we were in a meeting together, so nice to see you again.

In 2020, we witnessed one of the worst years on record for ransomware attacks and it could not have come at a more tenuous time for our society. With the onset of the pandemic, the Nation drastically shifted to remote work and services. While this yielded great benefits, it also provided a more expansive attack surface for cyber criminals. As COVID–19 cases increased, so did the number of devastating ransomware attacks. This trend represents an acceleration of what has impacted communities all across America for the past several years. In my district, for example, the Syracuse City School District and Onondaga County Library System previously fell victim to ransomware attacks that shut down their systems and halted the critical services that they provide.

I cannot emphasize this strongly enough: State and local governments and small businesses should leverage free services that CISA offers to help prevent and mitigate the scourge of ransomware attacks. CISA's guidance and services can help SLTT and small businesses take meaningful steps to increase the cyber-

secured posture of their networks. These preventative actions can make the difference between a devastating cyber event and business as usual.

We also must ensure CISA has the resources and capabilities to go toe-to-toe with sophisticated cyber criminals. CISA has made great strides to keep pace with the evolving threat, but there is must more that needs to be done.

The Fiscal Year 2021 National Defense Authorization Act provided important authorities that I advocated for that would ultimately allow CISA to rise to the challenge. But these must be met with resources to implement them. As I have continued to say, Congress needs to put CISA on a path to being a $5 billion agency.

I have been pleased to see CISA leveraging some of its newly established authorities, including State cybersecurity coordinators. These coordinators will be CISA's main point of contact embedded in each State government and be particularly important to ensuring it has a strong understanding of the needs of our local governments.

Additionally, I am happy to see CISA is fully leveraging its new authority provided by the DOTGOV Act to administer the top-level domain to provide secure and trustworthy dot-gov domains to State and local governments at no cost. CISA should also be doubling down on its efforts to stand up the Joint Cyber Planning Office to widen and streamline channels of communication between the Federal Government and industry.

We must think outside the box when it comes to slowing the rapid expansion of ransomware. Equipping State and local governments with the resources to bolster their defenses is an important first step. I am looking forward to working with Subcommittee Chairwoman Clarke and Chairman Thompson on the State and Local Cybersecurity Improvement Act to achieve that goal, but we can't stop there.

I look forward to hearing testimony from our witnesses on approaches that Congress should consider as we strive to tackle this problem once and for all. Recommendations from the Ransomware Task Force are a great place to start. But let us keep the pedal to the metal because we have a long way to go.

With that, Madam Chairwoman, I yield back.

[The statement of Ranking Member Katko follows:]

STATEMENT OF RANKING MEMBER JOHN KATKO

Thank you, Chairwoman Clarke, and Ranking Member Garbarino for holding this important hearing.

In 2020 we witnessed one of the worst years on record for ransomware attacks, and it could not have come at a more tenuous time for our society. With the onset of the pandemic, the Nation drastically shifted to remote work and services. While this yielded great benefits, it also provided a more expansive attack surface for cyber criminals. As COVID–19 cases increased, so did the number of devastating ransomware attacks. This trend represents an acceleration of what has impacted communities all across America for the past several years. In my district, the Syracuse City School District and Onondaga County Library System previously fell victim to ransomware attacks that shut down their systems and halted the critical services they provide.

I cannot emphasize this strongly enough: State and local governments and small businesses should leverage the free services the Cybersecurity and Infrastructure Security Agency (CISA) offers to help prevent and mitigate the scourge of ransomware attacks. CISA's guidance and services can help SLTT, and small busi-

nesses take meaningful steps to increase the cybersecurity posture of their networks. These left-of-attack preventative actions can make the difference between a devastating cyber event and business as usual.

We also must ensure CISA has the resources and capabilities to go toe-to-toe with sophisticated cyber criminals. CISA has made strides to keep pace with the evolving threat, but there's more to be done. The Fiscal Year 2021 National Defense Authorization Act provided important authorities that I advocated for that will ultimately allow CISA to rise to the challenge, but these must be met with resources to implement them. As I have continued to say, Congress needs to put CISA on a path to being a $5 billion agency.

I have been pleased to see CISA leveraging some of its newly-established authorities including State cybersecurity coordinators. These coordinators will be CISA's main point of contact embedded in each State government and be critically important to ensuring it has a strong understanding of the needs of our State and local governments. Additionally, I am happy to see CISA is fully leveraging its new authority provided by the DOTGOV Act to administer the top-level domain to provide secure and trustworthy .gov domains to State and local governments at no cost. CISA should also be doubling down on its efforts to stand up the Joint Cyber Planning Office to widen and streamline channels of communication between the Federal Government and industry.

We must think outside the box when it comes to slowing the rapid expansion of ransomware. Equipping State and local governments with the resources to bolster their defenses is an important step, and I'm looking forward to working with Subcommittee Chairwoman Clarke and Chairman Thompson on the State and Local Cybersecurity Improvement Act to achieve that goal. But we can't stop there. I look forward to hearing testimony from our witnesses on the innovative approaches that Congress should consider as we strive to tackle this problem once and for all. The recommendations from the Ransomware Task Force are a great place to start, but let's keep the pedal to the metal.

Chairwoman CLARKE. I thank you, Mr. Ranking Member, for your statement. Additional statements may be submitted for the record.

[The statements of Chairman Thompson and Honorable Jackson Lee follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

MAY 5, 2021

Good afternoon. I want to thank Chairwoman Clarke for holding this important hearing on the ransomware crisis facing our country.

Last fall, in my district, the Yazoo County School District paid $300,000 to a cybersecurity firm to recover data that was encrypted in a ransomware attack.

For a county of fewer than 30,000 people, that is a lot of money.

In fact, that is 1.5 percent of the school district's annual budget that had to be spent on just one incident.

Unfortunately, Yazoo County is not alone. School districts across the country have been forced to respond to ransomware attacks in the midst of the unprecedented challenges they have faced during this pandemic, where access to technology has been more important than ever.

To be clear, this is a National security issue.

We cannot expect school districts like Yazoo County to defend themselves alone when these attacks are coming from sophisticated criminal gangs based overseas that frequently have the tacit or even direct support of adversaries like Russia or North Korea.

And the harms these communities face are frequently not just financial.

Ransomware attacks have led to canceled school days, delayed medical procedures, and disruptions to emergency response services.

For these reasons, it is essential that we pass Chairwoman Clarke's State and Local Cybersecurity Improvement Act to ensure State, local, territorial, and Tribal governments get the assistance they need to defend their networks.

I am proud to be a cosponsor of this important legislation and look forward to working with Chairwoman Clarke and the bill's bipartisan group of supporters to get it enacted into law.

We cannot afford to wait any longer to provide the funding necessary to protect our State and local governments.

Fortunately, it is clear that the Biden administration has made addressing ransomware a priority.

From Secretary Mayorkas announcing DHS's 60-day sprint on ransomware to the Justice Department's new task force, the Executive branch is now demonstrating the coordinated approach that reflects the gravity of this threat.

This committee stands ready to work with them to ensure the resources and authorities are there to fulfill this critical mission.

The recently released Ransomware Task Force report provides numerous recommendations on how we can develop a cohesive approach to combatting ransomware.

I appreciate the hard work of the members of the Task Force in putting together this comprehensive document in just the last 3 months, reflecting the urgency of this growing crisis.

The report makes clear that despite the many challenges presented by cryptocurrencies and foreign adversaries that help disguise and protect ransomware criminals, there are important steps the Government can take to enhance defenses, improve information sharing, and collaborate with partners in the private sector and internationally to tack this problem.

These proposals have given Congress much to consider, and we are committed to ensuring that this issue remain a priority for Congress, so we can take meaningful action.

I am eager to hear more from the witnesses on these recommendations and how they envision DHS's role in implementing them.

I thank the witnesses for being here and again thank Chairwoman Clarke for her leadership on this issue and congratulate her on returning to chairing this important this subcommittee.

I look forward to continuing to work with her, along with the new subcommittee Ranking Member, Mr. Garbarino, on important cybersecurity issues like this one.

I yield back.

STATEMENT OF HONORABLE SHEILA JACKSON LEE

MAY 5, 2021

Chairwoman Yvette Clarke, and Ranking Member Andrew Garbarino, thank you for convening today's hearing on "Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis."

I thank today's witnesses:

- Maj. Gen. John Davis (Ret.), vice president and Federal chief security officer at Palo Alto Networks;
- Ms. Megan Stifel, executive director, Americas at the Global Cyber Alliance;
- Mr. Denis Goulet, commissioner, Department of Information Technology and chief information officer, State of New Hampshire (on behalf of the National Association of State Chief Information Officers); and
- Mr. Chris Krebs, former director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security.

I especially want to extend my thanks and appreciation to Mr. Christopher Krebs who has appeared before this committee on the topic of cybersecurity as the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

Your service to our Nation at a time when Russia worked to undermine the security of the 2020 election, just as it had done in the 2016 election was exemplary.

I regret that your work as head of CISA ended over your firm belief in being truthful to the American people regarding the cybersecurity of the election that Joe Biden won with over 7 million more votes than his opponent Donald J. Trump.

Cybersecurity is not something you can see or actively prove—it is established by each moment of each day that a network or computing device remains free of breaches by adversaries.

This hearing will provide Members the opportunity to engage with subject-matter experts on the problem of ransomware attacks.

The purpose of this hearing is to explore emerging trends in ransomware attacks and how the Government and private sector are working together to improve network defense.

In particular, the hearing will provide an opportunity to evaluate the recommendations made by the Ransomware Task Force report, released on Thursday of last week, which includes 48 recommendations directed at Federal agencies, State

and local governments, private-sector entities, and the international community to develop a comprehensive approach to confronting ransomware.

We know from our work on this committee that determined adversaries will spare little to succeed in breaching U.S. networks.

The goal of cybersecurity throughout the Federal Government must be to block adversaries when it is possible, detect and eradicate them quickly when it is not, and impose consequences to raise the costs and deter malicious behavior in cyber space.

For 4 years, Federal efforts to raise the National cybersecurity posture—across Federal networks, State and local governments, and the private sector—were stunted by a lack of steady, consistent leadership from the White House, leaving agencies to pursue piece-meal approaches to cybersecurity.

Congressional efforts to address the weaknesses in Federal cybersecurity include several Jackson Lee bills that include following measures introduced in the 117th Congress:

H.R. 119—Cyber Defense National Guard Act, which requires the Office of the Director of National Intelligence to report to Congress regarding the feasibility of establishing a Cyber Defense National Guard that may be activated during emergencies that affect the cybersecurity of the Nation or critical infrastructure.

H.R. 118—Cyber Vulnerability Disclosure Reporting Act, requires the Department of Homeland Security to submit a report describing the policies and procedures developed to coordinate the disclosure of cyber vulnerabilities. The report shall describe instances when these policies and procedures were used to disclose cyber vulnerabilities in the previous year. Further, the report shall mention the degree to which the disclosed information was acted upon by stakeholders.

H.R. 57, the DHS Cybersecurity Asset Protection of Infrastructure under Terrorist Attack Logistical Structure Act or the CAPITALS Act, which requires the Department of Homeland Security (DHS) to report to Congress on the feasibility of establishing a DHS Civilian Cyber Defense National Resource.

The goals of the Jackson Lee legislative efforts during the 116th Congress were to raise the baseline cybersecurity posture across the Federal and work with the private sector to reduce avoidable, opportunistic attacks and to refocus talent, time, and resources on preventing, detecting, and eliminating more sophisticated attacks.

The Raising the Nation's baseline cybersecurity posture will require a systemic, whole-of-Government approach to cybersecurity.

THE NEED TO TAKE ACTION

Ransomware is a form of cyber crime where criminal actors compromise a victim's computer systems, preventing access or threatening to release sensitive information if the victim does not provide a ransom payment.

In recent years, the number of ransomware attacks has increased significantly, affecting school districts, police departments, hospitals, and numerous businesses, among others.

In 2020, an estimated 2,400 governments, hospitals, and school districts were victims of ransomware attacks in the United States.

Victims made an estimated $350 million in ransomware payments in 2020, with an average payment of $312,493.

In the first quarter of 2021, the average monetary demand associated with a ransomware attack increased to $220,298, up 43 percent from the previous quarter.

While many businesses suffer significant losses due to disruptions from ransomware and the cost of remediation or making ransom payments, when criminals groups target Government entities or other critical infrastructure, the effects can pose significant risks to public safety.

For example, there were 560 ransomware attacks on U.S. health care facilities in 2020, in some cases causing delays in treatment for serious illnesses.

In a growing number of ransomware attacks, the perpetrators engage in "double extortion" where they threaten to release sensitive data publicly if a ransom payment is not made.

Last week, the Washington, DC police department was hit by a ransomware attack that included the release of detailed background reports on 5 current or former police officers and the threat to release files publicly.

Ransomware can be delivered in various ways, the majority of which utilize email. Ransomware are real, but computers aren't infected just by opening emails anymore.

Just opening an email to view it is safe now—although attachments & links in the email can still be dangerous to open.

Phishing is one of the most common methods of delivering ransomware. When a user downloads a malicious attachment within a phishing email which contains ransomware, all of the user's files are encrypted and made inaccessible until ransom is paid.

While it is not always possible to prevent a successful attack, engaging in general security best practices and implementing effective email protection can drastically reduce your risk.

This is why I introduce an amendment to last year's National Defense Authorization Act that implements a recommendation made by the Cyberspace Solarium Commission to require the Secretary of Homeland Security to develop a strategy to implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) standard across U.S.-based email providers.

I thank my Colleagues Congressmen Langevin, Gallagher, Katko, and Joyce for joining this bipartisan amendment to the fiscal year NDAA.

This amendment focused on the vulnerability of the internet's underlying core email protocol, Simple Mail Transport Protocol (SMTP), which was first adopted in 1982 and is still deployed and operated today.

However, this protocol is susceptible to a wide range of attacks including man-in-the-middle content modification and content surveillance.

The security of email has grown in importance as it has become in many ways the primary way that businesses, consumers, Government communicate.

The Solarium Commission's 75 recommendations are organized under 6 pillars:

(1) Reform the U.S. Government's Structure and Organization for Cyberspace;
(2) Strengthen Norms and Non-Military Tools;
(3) Promote National Resilience;
(4) Reshape the Cyber Ecosystem toward Greater Security;
(5) Operationalize Cybersecurity Collaboration with the Private Sector; and
(6) Preserve and Employ the Military Instrument of Power.

This amendment presented an opportunity to take a significant step forward in establishing a cybersecurity ecosystem that reinforces a cultural shift in how the Federal Government enforces norms that sustain cybersecurity.

Most recently, the Russian government infiltrated Government and critical infrastructure networks, in part, by executing a supply chain attack through the SolarWinds Orion platform.

In December, the Federal Government learned the Russian government had executed a malicious cyber campaign targeting Federal networks and certain critical infrastructure.

Russian hackers used a combination of traditional tactics, techniques, and procedures (e.g.: password guessing) and a supply chain attack to infiltrate targeted networks.

In a supply chain attack, malicious actors infiltrate a target network by exploiting security vulnerabilities in the network of a trusted partner to gain access to the targeted network.

In this case, one of the trusted partners was SolarWinds, a U.S.-based vendor whose Orion Platform provides network monitoring services to entities across the world, including the U.S. Government.

To execute the attack, hackers gained access to SolarWinds and injected malicious code into an Orion software update sent to customers in March 2020.

The malicious code created a back door in the affected network that caused the server to communicate with a U.S. IP address after a dormant period.

In response, hackers sent additional malicious code to some, but not all, affected networks.

Ultimately, the additional malicious code allowed hackers to access elevated credentials and move around a victim's network, monitoring activity and slowly taking data. To deceive security products on customers' networks, actors disguised their activity as normal network traffic and were able to persist through the creation of additional credentials from other applications.

A total of 18,000 SolarWinds customers downloaded the compromised version of Orion, but far fewer have identified activity beyond the creation of a backdoor.

Nearly 40 Federal agencies downloaded the compromised SolarWinds Orion update, but evidence of further compromise has only been detected at 9 Federal agencies to date. Agencies that downloaded the compromised Orion update continue to hunt for indicators of compromise.

It is important to note that about 30 percent of both Government and non-Government victims of the Russian cyber campaign had no direct connection with Solar Winds.

According to news reports, hackers also breached networks by "exploiting known bugs in software products, by guessing on-line passwords and by capitalizing on a variety of issues in the way Microsoft Corp.'s cloud-based software is configured."

Bugs can also be called Zero Day Events that if exploited could cost significant disruption in the function of application or services that rely in computers or remote computing services.

The SolarWind Orion exploit was not, from what we have learned thus far was not intended to damage or disrupt computing systems, it was designed to spy on networks and spread to other systems.

The SolarWinds campaign illustrates many of the shortcomings in the Federal Government's ability to monitor and respond to threats on private networks.

Because there is no overarching Federal law requiring private entities to report cybersecurity incidents, there is little public information on the number of victims that installed the infected versions of SolarWinds Orion or experienced second-stage intrusions.

The Cybersecurity and Infrastructure Security Agency should be empowered to more effectively coordinate and lead interagency cybersecurity and risk management activities.

Congress should provide CISA the authorities and budget that match its mission.

Over the past decade, the private sector has raised fair concerns about the value of many Federal cybersecurity programs and has used its concerns as an excuse for not fully participating, to the detriment of National cybersecurity efforts.

That must stop. The private sector has an important role to play to improve the Nation's cybersecurity posture and must step up.

Solving this cybersecurity challenge will require creativity from policy makers as we seek out new strategies to bolster security efforts for Federal and private-sector networks.

I look forward to working with the committee on a cybersecurity bill to address the issues raised in my statement.

I look forward to questions and answers with our witnesses.

I yield back.

Chairwoman CLARKE. I now welcome our panel witnesses.

Retired Major General John Davis is the vice president for the Public Sector at Palo Alto Networks and is also a co-chair of the Ransomware Task Force at the Institute for Security and Technology. Prior to joining the Palo Alto Networks, General Davis served as the senior military advisor for cyber to the undersecretary of defense for policy and served as the acting deputy assistant secretary of defense for cyber policy.

Ms. Megan Stifel is the executive director for the Americas at the Global Cyber Alliance and is also a co-chair of the Ransomware Task Force. Prior, Ms. Stifel served as a director for international cyber policy in the National Security Council at the White House and was an attorney in the National Security Division at the Department of Justice.

Mr. Denis Goulet is the commissioner of the Department of Information Technology for the State of New Hampshire and the current president of the National Association of State Chief Information Officers. Mr. Goulet also has nearly 30 years of private-sector IT experience in the sectors ranging from health care to manufacturing.

Finally, Mr. Chris Krebs, former director of the Cybersecurity and Infrastructure Security Agency, CISA, at the Department of Homeland Security.

Without objection, the witnesses' full statements will be inserted in the record. I now ask each witness to summarize his or her statement for 5 minutes beginning with General Davis.

STATEMENT OF MAJOR GENERAL JOHN A. DAVIS, U.S. ARMY (RETIRED), VICE PRESIDENT, PUBLIC SECTOR, PALO ALTO NETWORKS

Mr. DAVIS. Good afternoon. I am honored to appear before you today to discuss actionable policy solutions to address the unsustainable rise of ransomware. I would like to thank Chairman Thompson and Ranking Member Katko, Chairwoman Clarke and Ranking Member Garbarino for their leadership on this important issue. I offer my commitment to work in partnership with you and your staff to support the committee's actions to address this threat.

That the committee would hold this hearing shows that you see what we do, that ransomware is a profound and growing threat. Indeed, we believe that it has crossed a threshold. It is no long purely a criminal nuisance driven by a profit motive. Now it is impacting National security, economic stability, and public health and safety of the National and international community on a massive scale.

Unfortunately, the problem is getting worse. An analysis by the Palo Alto Networks' Unit 42 Threat Intelligence team concluded that the average ransom paid for organizations increased 171 percent year over year from 2019 to 2020. Adversary tactics are increasingly egregious. As mentioned earlier, in 2020, for instance, ransomware disproportionately impacted the health care sector as hospital systems struggled to cope with the COVID–19 pandemic.

This unsustainable trajectory compelled the creation of the Ransomware Task Force. Our goal was not to achieve an unrealistic outcome where all ransomware can be eliminated. Rather our objective is to proactively and relentlessly disrupt the ransomware business model and make ransomware a threat that can be more effectively managed through a series of coordinated actions which can be implemented by industry, Government, and civil society. In total, the report identifies 48 actions across 4 strategic goals: To deter ransomware attacks through a Nationally and internationally coordinated comprehensive strategy; to disrupt the ransomware business model and decrease criminal profits; to help organizations prepare for ransomware attacks; and to respond to ransomware attacks more effectively.

Our recommendations should be viewed as a set of collective mutually reinforcing actions that should be applied with continuous, coordinated, and overwhelming pressure. Some can be immediately pursued, some will require more time and creative policy solutions, including new legislation. I will focus today on 2 of the report's recommendations.

First, the United States should lead by example and execute a sustained, aggressive, whole-of-Government anti-ransomware campaign coordinated by the White House and in partnership with the private sector. The foundational step is recognizing that the nature of the ransomware challenge will require a massive team effort across Government, industry, academia, nonprofits, and the international community. This effort and our recommendations must be embraced at the highest levels of Government and industry as a policy priority and given sufficient resources. To this end, we are heartened to see recent actions at the Department of Homeland Security and the Department of Justice that signal elevated prioritization.

Second, we should develop a clear, actionable framework for ransomware mitigation, response, and recovery. We see a core responsibility to help all organizations better prepare. Improving the ability to prepare for and even prevent ransomware events from happening in the first place is, in my view, the single most important function in reducing this threat to a manageable level. The adage an ounce of prevention is worth a pound of cure is especially true in the case of ransomware because once you have been hit, you have already lost the battle and can only play a painful catch-up game.

Most organizations, regardless of size or security acumen, are aware of the threat, yet these organizations don't understand how to reduce their risk. An action we can take is the creation of an internationally-accepted framework that establishes clear steps to prevent or recover from attacks.

Finally, these recommendations serve as a foundation for other policy actions. For example, the task force recommends the creation of a cybersecurity grant for—a grant program for States where funding for ransomware prevention technologies could be unlocked through alignment to the best practice framework once it is established. This will enhance the resilience of local information systems and provide a much-needed modernization of security tools to prevent attacks.

Distinguished Members of this subcommittee, thank you again for the opportunity to testify today and I look forward to answering your questions.

[The prepared statement of Mr. Davis follows:]

PREPARED STATEMENT OF JOHN A. DAVIS

MAY 5, 2021

Chairwoman Clarke, Ranking Member Garbarino, and distinguished Members of the subcommittee, I am honored to appear before you today to discuss actionable policy solutions to address the unsustainable rise of ransomware. Thank you all for your leadership on this issue. I offer my commitment to work in partnership with you and your staff to support the subcommitte's oversight responsibilities on this issue.

That the committee would hold this hearing shows that you see what we do: That ransomware is a profound and growing cybersecurity threat. Indeed, ransomware has crossed a strategic threshold. It is no longer purely a criminal nuisance driven by a profit motive. Rather, it is now impacting National security, economic stability, and public health and safety of the National and international community on a massive scale.

Unfortunately, the problem is getting worse. An analysis by the Palo Alto Networks Unit 42 threat intelligence team concluded that the average ransom paid for organizations increased 171 percent year over year from 2019 ($115,123) to 2020 ($312,493). The highest-known paid ransom in 2020 doubled from the previous years ($5 million to $10 million). And adversary tactics are getting increasingly egregious. In 2020, for instance, ransomware disproportionately impacted the health care sector as hospital systems struggled to cope with the COVID–19 pandemic.

This unsustainable trajectory compelled Palo Alto Networks—and the broader ecosystem of collaborators that comprised the Ransomware Task Force—to take action. The Ransomware Task Force (RTF) is a public-private coalition of over 60 experts from Government, industry, nonprofits, and academia that came together to develop a comprehensive framework to tackle the ransomware threat. I am honored to represent the Task Force along with my colleague Megan Stifel at this hearing and discuss some of the key policy recommendations from the report the RTF released last week on April 29.

The goal of the RTF was not simply to help the world better understand ransomware; we are well past that point. Nor was it to achieve an unrealistic out-

come where all ransomware could be eliminated. Our objective was to proactively and relentlessly disrupt the ransomware business model through a series of coordinated actions which can be implemented by industry, Government, and civil society. In total, the report identifies 48 actions across 4 strategic goals.

1. Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy;
2. Disrupt the ransomware business model and decrease criminal profits;
3. Help organizations Prepare for ransomware attacks; and
4. Respond to ransomware attacks more effectively.

I will focus today on the report's recommendations that the United States should lead by example and execute a sustained, aggressive, whole-of-Government, intelligence-driven anti-ransomware campaign, coordinated by the White House, and that the United States should develop a clear, actionable framework for ransomware mitigation, response, and recovery, mapped to specific security capabilities organizations need to protect themselves.

Before turning to these points, I would like to introduce myself. As a reminder, I am here today in my capacity as a co-chair of the Ransomware Task Force. I am a retired U.S. Army Major General now serving as Vice President of Public Sector for Palo Alto Networks, where I am responsible for expanding cybersecurity and global policy initiatives for the international public sector and assisting governments and industry organizations around the world in preventing successful cyber attacks and protecting our digital way of life. Prior to joining Palo Alto Networks, I served as the senior military cyber advisor at the Pentagon and was appointed as the acting deputy assistant secretary of defense for cyber policy. Prior to this assignment, I served in multiple leadership positions in operational cyber assignments, special operations, and information warfare. These experiences provide me with a unique perspective on both the commercial cybersecurity marketplace as well as efforts under way across the U.S. Government to leverage technological innovation to solve critical cybersecurity challenges, including the threat of ransomware.

For those not familiar with Palo Alto Networks, we were founded in 2005 and have since become the world's largest cybersecurity company. We serve more than 80,000 enterprise and Government organizations—protecting billions of people—in more than 150 countries. We support 95 of the Fortune 100 and more than 71 percent of the Global 2000 companies, and are partnered with elite technology leaders.

Palo Alto Networks collaborates extensively with key stakeholders across the U.S. Government and with like-minded countries internationally on both policy and operational matters. For example, Palo Alto Networks is a member of the President's National Security Telecommunications Advisory Committee (NSTAC), providing industry counsel on National security policy and technology issues for the White House and other senior U.S. Government leaders; the Executive Committee of the Information Technology Sector Coordinating Council (IT–SCC), the principal entity for coordination between the Department of Homeland Security and IT sector; and the Defense Industrial Base Sector Coordinating Committee. Finally, we maintain robust threat intelligence-sharing partnerships with DHS, the intelligence community and across the international community to share technical threat data and collaborate to support Government and industry response to significant cyber incidents, like SolarWinds and Microsoft Exchange.

This commitment to meaningful collaboration with governments to tackle our shared cybersecurity goals is what compelled us to join the Ransomware Task Force. It has been an honor to be a part of this group and I have been humbled by the depth of passion and expertise this public-private partnership has brought to addressing this challenge. The diversity of thought, perspectives, and experience that the RTF reflects should give you confidence in the viability and immediacy of the recommendations articulated in the report at accomplishing these recommendations would lead to our overall shared strategic goals.

It's important to note that since its formation, the RTF has been deeply cognizant that we are not the first group to seek to tackle the ransomware issue. Many good initiatives have been stood up to focus on addressing cybersecurity and the threat of ransomware specifically. We stand on the shoulders of those efforts. The RTF never endeavored to replace that work—but instead consolidate and clarify the very best into a comprehensive strategic framework for action.

The RTF report recommendations are about dramatically reducing ransomware as a threat; there are no illusions about "solving ransomware." Instead, the report takes a practical approach to change the trajectory of this threat that has now crossed over a very dangerous threshold. We believe that our recommendations can reduce ransomware to a threat that can be more effectively managed like other threats that are dealt with through a practical risk management framework.

While I will highlight just a few of the report's key recommendations, I believe that the recommendations in the report should be viewed as a set of collective actions that should be applied with continuous, coordinated and overwhelming pressure. Some of these recommendations can immediately be pursued. Some will require creative policy solutions, including new legislation.

RTF Report Recommendation.—The United States should lead by example and execute a sustained, aggressive, whole-of-Government, intelligence-driven anti-ransomware campaign, coordinated by the White House.

A foundational step is recognizing that the nature of the ransomware challenge will require a massive effort to sustainably shift the trajectory. While I am a retired Army General, I will borrow a phrase from my Naval comrades to say that our report calls for an "all hands on deck" approach. No single organization, public or private, has all of the capabilities, capacities, skills, experience, resources, or authorities to act effectively in isolation.

It will take a team approach across Government, industry, academia, nonprofits, and the international community. This effort and our recommendations must be embraced at the highest levels of Government and industry as a policy priority and given sufficient resources. To this end, we are heartened to see recent actions at the senior levels of the Department of Homeland Security and Department of Justice that signal the elevated prioritization of addressing this issue on a National and international level. But much more can and must be done to elevate this to even higher organizational levels within the administration.

RTF Report Recommendation.—Develop a clear, actionable framework for ransomware mitigation, response, and recovery.

In addition to the need for greater strategic attention and coordination at the National policy levels, we also saw a core responsibility to help all organizations—States and localities, schools, and critical infrastructure like hospital systems—better prepare operationally for the threat of ransomware attacks.

Within the RTF, I was a co-chair of the Prepare Working Group. Improving the ability to prepare for and even prevent most ransomware events from happening in the first place is the single most important function in reducing this threat to a manageable level. Building on best practices that have proven to be successful, clarifying and consolidating them, and making them easily accessible at appropriate levels is one of the most powerful tools we can employ. The adage "an ounce of prevention is worth a pound of cure" is especially true in the case of ransomware because, once you have been hit, you have already lost the battle and can only play catch up.

Most organizations, regardless of size or security acumen, are aware of the threat of ransomware. But most are not similarly empowered with adequate knowledge to quantify how finite resources can be applied to reduce their risk to ransomware threats specifically. We need to bridge the communications gap between IT and security professionals and senior organizational leadership. We need organizations to stop thinking about ransomware as a niche cybersecurity issue but instead as a core business continuity risk that must be managed in the same way as other physical disruptions.

The RTF saw the current State of awareness around ransomware as similar to the environment prior to 2014, when no authoritative compilation of best practices existed for cybersecurity generally. NIST responded by leading a multi-stakeholder process to create the *Framework for Improving Critical Infrastructure Cybersecurity*. In a similar way, the single most impactful measure we can take to help organizations is the creation of an internationally accepted framework that establishes clear actionable steps to prevent ransomware, and recover from it if prevention is not successful.

Of course, while technology isn't the only category associated with building this framework, it is certainly an important arrow in the quiver. Ransomware prevention technologies exist today and have demonstrated success. However, these technologies are not widely adopted. Coming from the cybersecurity industry, I have personally witnessed both traditional and emerging technologies that have demonstrated success in preventing ransomware attacks. Effective technologies include Endpoint or Extended Detection and Response (EDR/XDR) with automated behavioral analytics, fileless protections and deceptive technologies that stage objects as decoys or deploy decoy documents. These tactics employ automation and advanced analytics to flag modification to files and automatically prevent the ransomware encryption process. There are also cloud-based capabilities to launch unknown processes or applications in a container, which prevents malicious software or command and control channels from interacting with an organization's core network.

More traditional technologies at the network level include those that monitor and block common ransomware methods, such as Remote Desktop Protocol (RDP),

phishing protections, capabilities that limit access to unknown or risky domains, and Secure Socket Layer (SSL) decryption to observe and scan content as it traverses the network. Finally, the traditional capabilities such as Uniform Resource Locator (URL) filtering, Domain Name System (DNS) security, Intrusion Prevention Systems (IPS) and sandboxing capabilities provide protections against many common ransomware tactics, techniques, and procedures.

Once the proposed ransomware framework's baseline security standards are established, it will be critical to map those standards to the specific security capabilities that organizations need to protect themselves. The creation of framework-aligned ransomware prevention reference architectures using industry leading technologies, consistent with the on-going work at NIST's National Cybersecurity Center of Excellence, would be helpful toward this end.

Finally, these baseline best practices can also serve as a foundation for a number of potential policy actions to raise the bar of security across critical infrastructure and Government. To this end, the RTF report suggests several incentives for entities that demonstrate a commitment to maturing their capabilities in alignment with the ransomware framework. For example, the report recommends the creation of a cybersecurity grant program for States and localities, where funding to procure ransomware-prevention-focused security technologies could be unlocked through demonstrated alignment to the established best practice framework. Dedicated funding—aligned to strong cybersecurity planning and continuous vulnerability assessments—will enhance the resilience of State and local information systems, and provide a much-needed modernization of the security tools these governments use to prevent ransomware attacks. Opening up opportunities for multi-State grants will further drive innovation, security, and efficiency.

Chairwoman Clarke, Ranking Member Garbarino, and distinguished Members of the subcommittee, thank you again for the opportunity to testify today. I look forward to answering any questions you may have.

Chairwoman CLARKE. Thank you. I now recognize Megan Stifel to summarize her statement for 5 minutes.

STATEMENT OF MEGAN H. STIFEL, EXECUTIVE DIRECTOR, AMERICAS, GLOBAL CYBER ALLIANCE

Ms. STIFEL. Chairwoman Clarke, Ranking Member Garbarino, Members of the subcommittee, thank you for the opportunity to testify today on the growing threat ransomware poses to our homeland and National security. My name is Megan Stifel and I am the executive director, Americas, at the Global Cyber Alliance, an international nonprofit organization dedicated to providing practical solutions to reducing cybersecurity risks.

Like John, I appear before you today as co-chair of the Ransomware Task Force, a group of more than 50 organizations that convened with the Institute of Security and Technology and gathered over the past 4 months to develop a comprehensive framework to reduce the risk of ransomware. Last week the task force published a report outlining 5 priority recommendations to achieve 4 goals, as noted with a series of 48 total recommendations. I will focus my testimony today on 3 of these recommendations.

First, the need for a coordinated international diplomatic and law enforcement effort to prioritize ransomware, supported in the United States by a whole-of-Government strategy.

Second, the need for enhanced information to support and enable this effort, including the development of a ransomware framework to help organizations better prepare for and respond to ransomware.

Third, the establishment of cyber response and recovery funds and other assistance to support ransomware response and other cybersecurity activities.

As the Members of the subcommittee well know, the scope and scale of ransomware has grown exponentially over the past year. Payments in the $40,000 range in 2019 quadrupled to $170,000 on average in 2020. Recent reports indicate that some payments have stretched to the millions while demands have stretched to the tens of millions. But as also noted, not the size of payments just grew, but also the number of organizations targeted. Twenty-four hundred U.S.-based Government health care facilities and schools were known to have been targeted in 2020 by ransomware. The actual number who were affected potentially may be much higher.

In addition to holding access to data hostage, ransomware hackers now threaten to publish the data they obtained from the victims' networks. According to one report in the fourth quarter of 2020, 70 percent of reported ransomware attacks threatened to release the data. Ransomware is, plain and simple, 21st Century extortion.

These figures illustrate that in just a few years ransomware has grown from a nuisance to a National security threat. Organizations around the world have been targeted, but as has also been well established, ransomware actors operate from safe havens, countries whose governments are mostly unwilling as well as unable to assist in efforts to bring them to justice. As such, without significantly limiting the ransomware attack at scale, there is little guarantee it will not simply emerge elsewhere, presenting an on-going risk to the global community.

The Ransomware Task Force convened in order to address this growing international challenge. Its breath influenced the task force's first priority recommendation. Specifically, the coordinated international diplomatic and enforcement efforts make clear that ransomware is an international and National security and law enforcement priority, and that an international coalition be established to combat it.

Governments must also develop comprehensive, resourced strategies that use both carrots and sticks to reduce the number of countries providing safe havens. But as the task force's other recommendations make clear, governments must also work collaboratively together and with the private sector to share information, jointly investigate, and bring these actors to justice or otherwise eliminate their ability to operate with impunity.

For the United States, the task force recommends that this effort be led by a whole-of-Government strategy out of the White House. This strategy should also include a Ransomware Task Force to coordinate a Nation-wide campaign against ransomware and identify and pursue opportunities for international collaboration. This task force should also collaborate closely with private-sector organizations that can help defend and disrupt ransomware operations, such as security vendors, platforms, ISAOs, and cybersecurity nonprofits.

Second, better information is necessary to enable this collective international action. It is important to emphasize we are not talking about more information sharing of indicators of compromise. Both the scope and quality of information must improve. For example, IOCs should be tied to ransomware incidents and this information must get quickly into the hands of those who can use it within

the Government as well as outside it. IOCs must also be supplemented with additional information, including payments.

Better information, however, is necessary, but insufficient to fully combat this threat. Organizations, both their leadership as well as their operational—in operational roles need to understand that ransomware is a real and relevant threat. They need better guidance on how to prioritize mitigation efforts, especially given their limited resources.

To address this gap, the task force recommends that a framework be developed to help organizations better prepare for and respond to ransomware attacks, together with materials to support framework implementation such as tool kits and other how-to resources. The Global Cyber alliance, and other organizations, I am sure, is ready to add such guidance to our existing resources to assist organizations in reducing their risk.

Finally, additional resources for implementation are essential to the success of the ransomware framework and through it the disruption of the ransomware business model. The task force, therefore, recommends that governments establish response and recover funds. The task force believe the ability of these funds will help reduce the number of victims electing to pay the ransom demand. As an incentive, organizations could be required in order to access such funds to demonstrate a use of the ransomware framework to ensure a commitment to a baseline level of cybersecurity.

In addition, the task force recommends that more grant funding be available. For example, Homeland Security Preparedness Grants could be expanded to address cybersecurity threats.

On a personal note, I would like to emphasize the importance of these grants. A dollar spent to prevent crime will be more effective than a dollar spent to recover from it.

In closing, I want to highlight the essential role nonprofits played in developing the task force's recommendations and that they can play in their implementation. Nonprofits develop policy recommendations, support information sharing, and, in the case of GCA, provide guidance on the implementation of established cybersecurity best practices, including to combat ransomware. The task force offered a range of actions that could be taken building on these capabilities to stem the burgeoning ransomware threat.

Nonprofits depend on contributions from a range of stakeholders to fulfill their unique and important roles. Now more than ever it is critically important that all stakeholders take collective action to combat this threat.

Thank you again for the opportunity to testify today. I welcome your questions.

[The prepared statement of Ms. Stifel follows:]

PREPARED STATEMENT OF MEGAN H. STIFEL

MAY 5, 2021

Chairwoman Clarke, Ranking Member Garbarino, Members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation, thank you for the opportunity to testify today on the growing threat ransomware poses to our homeland and National security.

My name is Megan Stifel, and I am the executive director, Americas, at the Global Cyber Alliance (GCA). GCA is an international nonprofit organization dedicated to providing practical solutions to reduce cybersecurity risk. I appear before you today

as a co-chair of the Ransomware Task Force, convened by the Institute for Security and Technology, and comprised of over 50 organizations that gathered over the past 4 months to develop a comprehensive framework to reduce the risk of ransomware. Last week the Task Force published a report outlining its recommendations, including 4 goals and 5 priority recommendations, with a series of supporting actions constituting 48 total recommendations. The priority recommendations include the need for sustained, coordinated collective action among governments, industry, academia, and nonprofits to meaningfully reduce the ransomware threat.

I will focus my testimony today on 3 of these priority recommendations. First is the need for a coordinated, international diplomatic and law enforcement effort to prioritize ransomware, supported in the United States by a comprehensive whole-of-Government strategy. Second is the need for enhanced information to support and enable this effort, including the development of a ransomware framework to help organizations better prepare for and respond to ransomware. And third is the establishment of Cyber Response and Recovery Funds and other assistance to support ransomware response and other cybersecurity activities.

As Members of this subcommittee know well, the scale and scope of the ransomware challenge has grown exponentially over the past year. In 2019 the average ransomware payment was $43,593; by the end of 2020 it had quadrupled to $170,696.[1] Recent reports indicate some payments have stretched to the millions, while demands have reached the tens of millions.[2] But not just the size of ransom payments grew, so too did the number of organizations targeted, including hospitals and schools. In 2020, nearly 2,400 U.S.-based government, health care facilities, and schools were known to have been targeted with ransomware,[3] with the actual number affected potentially much higher. In addition to holding access to data hostage, ransomware actors are now threatening to publish data they have obtained from the victim's networks. According to Coveware, in the third quarter of 2020, 50 percent of ransomware attacks involved a threat to release data. That figure rose to 70 percent in the fourth quarter of 2020. Ransomware is plain and simple 21st Century extortion.

These figures illustrate that in just a few years ransomware has grown from a nuisance to a National security threat. And it is not just a problem for the United States. Organizations around the world have been targeted by ransomware.[4] As has also been well established, these threat actors operate from safe havens, countries whose governments are mostly unwilling as well as unable to support efforts to bring them to justice. Given the size of this threat, reducing its impact in one country is not possible without the assistance of others. Likewise, even if the United States and partner nations reduce ransomware in their own jurisdictions, without significantly limiting this threat at scale, there is little guarantee it will not simply emerge elsewhere, presenting an on-going risk to the global community.

AN INTERNATIONAL, COLLABORATIVE EFFORT MUST FORM TO REDUCE THE RANSOMWARE THREAT

The Ransomware Task Force convened to address this growing international challenge. The breadth of the challenge informed the Task Force's first priority recommendation. Specifically, coordinated international diplomatic and enforcement efforts must make clear that ransomware is an international national security and law enforcement priority and that an international coalition should be developed to combat it. Governments should also develop a comprehensive, resourced strategy that uses both carrots and sticks to reduce the number of countries providing safe havens. In doing so, governments can build on the 2020 G7 finance minister's statement in further signaling publicly the urgency of this threat. But as the Task Force's other recommendations make clear, governments must also work collaboratively among themselves and with the private sector to share information, jointly investigate, and bring these actors to justice or otherwise eliminate their ability to operate with impunity.

---

[1] Coveware, "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," February 1, 2021, available at: *https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020.*

[2] CNBC, "The extortion economy: Inside the shadowy world of ransomware payouts," April 6, 2021, available at: *https://www.cnbc.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html.*

[3] Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, available at: *https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/*.

[4] Sophos, "The State of Ransomware 2020," May 2020, available at: *https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf.*

For the United States, the Task Force recommends that this collective and collaborative action be driven by a whole-of-Government strategy, led by the White House. Such a strategy should also include a Joint Ransomware Task Force to coordinate an on-going, Nation-wide campaign against ransomware and identify and pursue opportunities for international cooperation. This joint interagency task force should be empowered at the appropriate levels to use all instruments of National power, and it should prioritize ransomware threats to critical infrastructure. In conducting its work, the interagency task force should also collaborate closely with relevant private-sector organizations that can help defend against and disrupt ransomware operations, such as security vendors, platform providers, information sharing and analysis organizations, and cybersecurity nonprofits.

The Task Force further recommends the development of a Ransomware Threat Focus Hub that can also support existing, informal efforts. The Hub can serve as a central, organizing node for informal networks and collaboration of a sustained public-private anti-ransomware campaign. In addition, to support the Hub's and its participants' ability to disrupt the ransomware life cycle, the Task Force also recommends that the Departments of Justice and Homeland Security provide further clarity on the scope of defensive measures entities may undertake pursuant to the Cybersecurity Information Sharing Act of 2015.

THE SCOPE AND QUALITY OF INFORMATION ABOUT RANSOMWARE MUST IMPROVE

In order to develop and support this international strategy and its domestic elements, and through such a strategy eliminate safe havens, members of the Task Force believe that better information is necessary to enable this collective action. It is important to emphasize that this is not just more information sharing of cyber threat indicators, or indicators of compromise (IOCs), as they are also called. Both the scope and quality of information must improve. For example, IOCs should be tied to ransomware incidents, and this information must get into the hands of those who can use it—within the government as well as outside it. IOCs also need to be supplemented with additional information about ransomware incidents, including payments.

Due to the limited and inconsistent nature of information about ransomware incidents, the Ransomware Task Force also recommends that national governments encourage organizations that experience a ransomware attack to voluntarily report the incident. Furthermore, the Task Force recommends that should a victim elect to pay the ransom they be required to share details with the government in advance of such payment. At a minimum, the notification should include the ransom date, demand amount, and payment instructions (e.g., wallet number and transaction hashes). Gathering and analyzing this information is essential not just for law enforcement but also for incident responders and insurers, who can deploy additional analytic tools that may help cybersecurity firms prevent the next incident as well as allow insurers to pursue payment recovery, including through subrogation.

This information is necessary but insufficient to fully combat this threat. Organizations, both their leadership as well as those in operational roles, need to better understand that ransomware is a real and relevant threat and have better guidance on how to prioritize mitigation efforts given limited resources. To address this knowledge gap, the Task Force recommends that a framework be developed to help organizations better prepare for and respond to ransomware attacks, together with materials to support framework implementation such as tool kits and other how-to resources. Importantly, this framework should include customized recommendations based on each organization's current capacity to implement the recommendations. Following the success of the Cybersecurity Framework, the Task Force recommends that the National Institute of Standards and Technology convene an effort to develop this ransomware framework, in collaboration with international counterparts. The development of tool kits and other how-to materials are a necessary complement to ensure wide-spread adoption of the ransomware framework. GCA (and other organizations, I am sure) is ready to add such guidance to our existing resources to assist organizations in reducing their ransomware risk.[5]

ESTABLISHING RESPONSE AND RECOVERY FUNDS AND EXPANDING GRANT AVAILABILITY CAN SUPPORT VICTIMS AND DISRUPT THE RANSOMWARE BUSINESS MODEL

Resources for implementation are essential to the success of the ransomware framework and through it the disruption of the ransomware business model. To address this need, the Task Force recommends that governments establish Response

[5] Global Cyber Alliance Blog, "Combatting Ransomware: A Call to Action," April 29, 2021, available at: *https://www.globalcyberalliance.org/combatting-ransomware-a-call-to-action/*.

and Recovery Funds. These funds should cover the cost, for example, of restoring systems for victims that serve essential functions including local governments as well as critical national functions. The Task Force believes that the availability of these funds will help reduce the number of victims electing to pay the ransom demand. As an incentive for organizations to invest in cybersecurity, governments could consider requirements to access the fund, such as demonstrating use of the ransomware framework to ensure a commitment to a baseline level of cybersecurity.

In addition, the Task Force recommends that more grant funding be available to use for cybersecurity. For example, Homeland Security Preparedness Grants could be expanded to address cybersecurity threats. Additional grants, along the lines established by the Help America Vote Act, could also be made available to States through which they could manage delivery of funds to municipalities. Not only would these investments reduce cybersecurity risks, they will also enhance State, local, Tribal, and territorial resilience as upgrading software and hardware are often the most cost-effective security investments organizations can make. As with Response and Recovery Funds, access to these grants could be conditioned upon demonstrated alignment with the ransomware framework following its development. Elements of the State and Local Cybersecurity Improvements Act, which passed the House of Representatives last session, could serve as a baseline effort to address these recommendations.

On a personal note, I'd like to emphasize the importance of these grants. A dollar spent to prevent a crime will be more effective than a dollar spent to recover from it. Moreover, some grant funding should be focused on prevention mechanisms that can be used by many and work at scale rather than requiring every grantee to reinvent the wheel.

CONCLUSION

Combating ransomware is important because it is threatening large sections of the U.S. and global economy including health care services and schools. Left unchecked, its rapid growth is threatening national security, and payments associated with it are supporting a number of societal harms including human trafficking and the development of weapons of mass destruction. To combat this challenge, the Ransomware Task Force believes that the previously described recommendations together with other actions detailed in its report will, when implemented collectively, significantly reduce ransomware in the coming years.

In cybersecurity it is not often the case that one player can also fulfill another's role—we each have unique roles and bring unique capabilities. The Task Force offered a range of actions that could be taken building upon these unique capabilities, including with nonprofit resources, to stem this burgeoning threat. In closing, I want to highlight the essential role nonprofits played in the development of the Task Force's recommendations and that they can play in its implementation. Nonprofits may develop policy recommendations, support information sharing, and in the case of GCA, provide guidance on the implementation of established cybersecurity best practices including to combat ransomware. Nonprofits depend on contributions from a range of stakeholders to fulfill their unique and important roles. What is most important is that more action be taken by all stakeholders.

Thank you again for the opportunity to testify today. I welcome your questions and comments.

Ms. RICE. Thank you for your testimony. I now recognize Mr. Goulet to summarize his statement for 5 minutes.

STATEMENT OF DENIS GOULET, COMMISSIONER, DEPARTMENT OF INFORMATION TECHNOLOGY, AND CHIEF INFORMATION OFFICER, STATE OF NEW HAMPSHIRE, AND PRESIDENT, NATIONAL ASSOCIATION OF CHIEF INFORMATION OFFICERS, TESTIFYING ON BEHALF OF THE NATIONAL ASSOCIATION OF CHIEF INFORMATION OFFICERS

Mr. GOULET. Thank you, Chairwoman Clarke, Ranking Member Garbarino, distinguished Members of the subcommittee, for inviting me today to speak on the cybersecurity challenges facing——

Ms. RICE. Can everyone hear? Mr. Goulet? Mr. Goulet? Can you either get closer to the microphone? We are having a hard time hearing you.

Mr. GOULET. Better?

Ms. RICE. Yes, if you could just speak up, that would be great.

Mr. GOULET. Thank you, Chairwoman Clarke, Ranking Member Garbarino, distinguished Members of the subcommittee, for inviting me today to speak on the cybersecurity challenges facing State and local governments. As commissioner of the Department of Information Technology in New Hampshire and the president of NASCIO, I am grateful for the opportunity to discuss cybersecurity, efforts to mitigate ransomware attacks, as well as highlight the vital role that State information technology agencies play in providing critical citizen services, ensuring the continuity of Government.

Cybersecurity has remained the top priority for State CIOs for the past 8 years. My State and across the country we are observing a shift among Government leaders treating cybersecurity as a continuity of Government issue. But while we used to be concerned with theft of data and personally identifiable information, the nature and scope of cyber attacks today are aimed at crippling the functioning of our Government. Recent attacks on water treatment facilities and hospital systems have shown us how these incidents have progressed from digital consequences to sophisticated strikes designed to threaten the health and safety of our Nation's citizens.

We have observed that ransomware incidents are disproportionately affecting the LTT part in State, local, territorial, and Tribal governments. The question of why the Federal Government is not contributing to the cybersecurity of the States is straightforward as States are the primary agents for the delivery of a vast array of Federal programs and services.

A lack of adequate resources for cybersecurity continues to be the most significant challenge facing State and local governments. State CIOs are tasked with additional responsibility, including providing cybersecurity assistance to local governments, doing so with shortages in both funding and cyber talent. The 2020 NASCIO Cybersecurity Study found that only 36 percent of States and territories have a dedicated cybersecurity budget and nearly a third have seen no growth in those budgets.

Almost all CIOs are directly responsible for the cybersecurity in their State and have initiatives to improve their cybersecurity posture. These programs are crucial as Congress considers the implementation of a cybersecurity grant program for State and local governments. Key elements include a centralized approach to cybersecurity; adoption of a cybersecurity strategic plan and framework; development of a cyber disruption response plan; and implementation of regular security awareness training for employees and contractors.

For the past decade, NASCIO has advocated for a whole-of-State approach to cybersecurity. We define this approach as collaboration among State agencies and Federal agencies, local governments, the National Guard, the education sector, critical infrastructure providers, and private-sector partners. By approaching cybersecurity as a team sport, information is widely shared and each stakeholder has a clearly-defined role to play.

My colleagues across the country have significantly increased our involvement in fighting ransomware, especially with our local gov-

ernment partner. We have taken on additional responsibilities and incurred new expenses while continuing to face an unrelenting cyber threat environment.

I am truly concerned about how crucial IT and cybersecurity will be funded in coming months and years. While COVID relief legislation has provided opportunities for some States to improve their cybersecurity posture, the pandemic has amplified vulnerabilities in State and local networks.

I know I speak for all of my colleagues around the country when I say that a dedicated Federally-funded cybersecurity grant program, like the State and Local Cybersecurity Improvement Act, is overdue and will strengthen our ability to defend ourselves from cyber attacks.

Since the Act would also require State legislatures to match a portion of Federal grant funds, it would provide an increased incentive for State legislatures to make cyber an on-going priority in every State's budget.

I look forward to continuing to work with the Members of this subcommittee in the creation of a program to improve our cybersecurity. This concludes my formal testimony. I look forward answering your questions. Thank you.

[The prepared statement of Mr. Goulet follows:]

PREPARED STATEMENT OF DENIS GOULET

WEDNESDAY, MAY 5, 2021

Thank you, Chairwoman Clarke, Ranking Member Garbarino, and the distinguished Members of the subcommittee for inviting me today to speak on the numerous cybersecurity challenges facing State government that have been amplified during the COVID–19 pandemic. As commissioner for the Department of Information Technology in New Hampshire and the president of the National Association of State Chief Information Officers (NASCIO), I am grateful for the opportunity to discuss cybersecurity, efforts to mitigate ransomware attacks, as well as highlight the vital role that State information technology (IT) agencies have played in providing critical citizen services and ensuring the continuity of government throughout the current public health crisis.

STATE CYBERSECURITY OVERVIEW AND CHALLENGES

As president of NASCIO, I am honored to represent my fellow State chief information officers (CIOs) and other State IT agency leaders from around the country here today. While some of my testimony will be based on my experiences as CIO in New Hampshire for the past 6 years, I will also be providing the members and staff of the subcommittee with National trends and data from NASCIO's 2020 State CIO Survey and the 2020 Deloitte-NASCIO Cybersecurity Study.

It may come as little surprise to you that cybersecurity has remained the top priority for State CIOs for the past 8 years. In my State and across the country, I have seen a palpable shift among government leadership that IT and cybersecurity are not simply regarded as a technology problem but a key tenet to the continuity of our government. While we used to be concerned only with the theft of data and personally identifiable information (PII), the nature and scope of cyber attacks today are aimed at crippling the entire functioning of our government. Recent attacks on water treatment facilities and hospital systems have shown us how these incidents have progressed from digital consequences to sophisticated strikes designed to threaten the health and safety of our Nation's citizens.

The threat environment we face is incredibly daunting with State cyber defenses repelling an estimated 50 to 100 million potentially malicious probes and actions every day. State and local governments remain attractive targets for cyber attacks as evidenced by dozens of high-profile and debilitating ransomware incidents. The financial cost of these attacks is truly staggering with a recent report from Emsisoft finding that ransomware attacks in 2019 impacted more than 960 government agen-

cies, educational institutions, and health care providers at a cost of more than $7.5 billion.

Lack of adequate resources for cybersecurity has been the most significant challenge facing State and local governments, even prior to the COVID–19 pandemic. As State CIOs are tasked with additional responsibilities, including providing cybersecurity assistance to local governments, they are asked to do so with shortages in both funding and cyber talent.

The question of why the Federal Government should be contributing to the cybersecurity of the States is straightforward as States are the primary agents for the delivery of a vast array of Federal programs and services. A lack of budgeting at the State level for cybersecurity is also a significant impediment. The 2020 Deloitte-NASCIO Cybersecurity Study found that only 36 percent of States and territories have a dedicated cybersecurity budget and nearly a third have seen no growth in those budgets. The study also found that State cybersecurity budgets are typically less than 3 percent of their overall IT budget, which is far less than Federal agencies and financial institutions.

NASCIO has long encouraged State government officials to establish a dedicated budget line item for cybersecurity as a subset of the overall technology budget. While the percentage of State IT spending on cybersecurity may be much lower than that of private sector industry and Federal agency enterprises of similar size, the line item can help State IT leaders provide the State legislature and Executive branch leaders the right level of visibility into State cybersecurity expenses in an effort to rationalize spending and raise funding levels. State legislation could demand visibility into cyber budgets at both the State and individual agency levels. In addition, the Deloitte-NASCIO Cybersecurity study results indicate that Federal and State cybersecurity mandates, legislation and standards with funding assistance result in more significant progress than those that remain unfunded. While we still have a long way to go, I greatly appreciate legislative efforts by numerous Members of this subcommittee to encourage State legislators to begin budgeting for cybersecurity.

A WHOLE-OF-STATE APPROACH

More than 90 percent of CIOs are responsible for their State's cybersecurity posture and policies. In collaboration with their chief information security officers (CISOs), whose role has expanded and matured in recent years, CIOs have taken numerous initiatives to enhance the status of the cybersecurity program and environment in their States. I believe these initiatives are also fundamentally crucial as Congress considers the implementation of a cybersecurity grant program for State and local governments. Some of these key tenets include: A centralized approach to cybersecurity, the adoption of a cybersecurity strategic plan and framework based on the NIST Cybersecurity Framework, the development of a cyber disruption response plan and the implementation of regular security awareness training for employees and contractors.

One key initiative is the whole-of-State approach to cybersecurity, which NASCIO has advocated for over the past decade. We define the whole-of-State approach to cybersecurity as collaboration among State agencies and Federal agencies, local governments, the National Guard, education (K–12 and higher education), utilities, private companies, health care, and other sectors. By approaching cybersecurity as a team sport, information is widely shared and each stakeholder has a clearly defined role to play when an incident occurs. Additionally, many States who have adopted the whole-of-State approach have created State-wide incident response plans. According to our 2020 CIO survey, more than 79 percent of State CIOs have implemented a whole-of-State approach in their States, are in the process of implementing or planning to implement.

Crucially, numerous State IT agencies are conducting cyber incident training and incident response exercises with these partners to ensure they are able to quickly operationalize their incident response plans. One example of this type of training is the inaugural State-wide Cyber Summit for Local Governments that we held in New Hampshire earlier this spring. We had over 250 local government attendees from towns, cities, counties, and school districts with Federal participants from CISA and the Secret Service. Regular cyber exercises not only increase cyber awareness across all levels of the State but foster key relationships and trust among officials allowing for a more successful and rapid response when an incident occurs.

In August 2019, more than 2 dozen local governments, education institutions, and critical infrastructure systems in Texas were struck by debilitating and coordinated ransomware attacks. However, it was the successful collaboration and cooperation among Federal, State, and local officials—a whole-of-State approach combined with

a detailed cyber incident response plan—that prevented these attacks from succeeding. In fact, as Amanda Crawford, Texas CIO and executive director of the Texas Department of Information Resources, testified before the Senate Homeland Security and Governmental Affairs Committee in February 2020, all impacted entities were remediated within 1 week after the attacks.

STATE AND LOCAL COLLABORATION

As the Texas ransomware attacks illustrate, under-resourced and under-staffed local governments continue to remain an easy target for cyber attacks. Due to the combination of a whole-of-State approach to cybersecurity and the proliferation of numerous high-profile ransomware attacks across the country, State CIOs have significantly increased collaboration with local governments to enhance their cybersecurity posture and resilience. In fact, more than 76 percent of CIOs reported increased collaboration and communication with local governments in the last year.

In 2020, NASCIO released a research paper with the National Governors Association focused on State and local collaboration titled "Stronger Together." As Congress considers the components of a State and local cybersecurity grant program, I would urge you to incorporate some of the conclusions from that paper. This includes encouraging States to continue building relationships with local governments and helping States raise awareness for IT and cybersecurity services offered to local governments.

Additionally, Congress should assist State and local governments with more easily purchasing cybersecurity tools and services through existing models at the Federal level. Streamlining the procurement of cybersecurity services would also expedite a currently bureaucratic process and result in significant cost savings.

PARTNERSHIP WITH DHS CISA

In terms of partnerships with Federal agencies, I do want to highlight State IT's growing partnership with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). While this relationship is still in its infancy, CIOs and CISOs appreciate the cybersecurity resources, services, and guidance provided by CISA. NASCIO has and will continue to support efforts to define CISA's roles and responsibilities more clearly in assisting State and local governments. We've also endorsed Federal legislation to increase CISA's resources within each State. This includes the recent passage and enactment of S. 3207, the Cybersecurity State Coordinator Act, which will ensure greater continuity between the efforts of States and the Federal Government. It will also provide a stronger State voice within CISA, helping them to better tailor their assistance to States and localities.

Additionally, NASCIO was a strong advocate of the DOTGOV Act, which was included in the omnibus Government funding bill signed into law in December 2020. The DotGov Act transferred ownership of the DotGov Program from the General Services Administration to CISA, which officially took place last month, and reinforced the important cybersecurity aspect of domain registration. I want to praise CISA and the DotGov Office for their announcement last week to waive all fees for new DotGov registrations. The $400 annual fee had been a significant barrier of adoption for local governments, who remain most vulnerable to misinformation and disinformation campaigns. With less than 10 percent of all eligible local governments currently on DotGov, NASCIO looks forward to continuing our work with CISA to better improve the cybersecurity of local governments. Now more than ever, it is essential to ensure the American people are receiving accurate and authoritative information from their Government websites.

DEDICATED CYBERSECURITY FUNDING FOR STATE AND LOCAL GOVERNMENTS

I would again like to reiterate my appreciation to this subcommittee for its attention to cybersecurity issues impacting State and local governments. The 116th Congress focused significantly on these issues and introduced numerous pieces of legislation endorsed by NASCIO. In particular, I look forward to continuing to work with the Members of this subcommittee to ensure the passage of a State and local cybersecurity grant program.

Currently, cybersecurity spending within existing Federal grant programs, including the Homeland Security Grant Program, has proven challenging in the face of declining Federal allocations, increased allowable uses and a strong desire to maintain existing capabilities that States have spent years building. In fact, less than 4 percent of all Homeland Security Grant Program funding has been allocated to cybersecurity over the last decade.

NASCIO urges the reintroduction and passage of the bipartisan State and Local Cybersecurity Improvement Act, a $400 million annual grant program for State and

local governments to strengthen their cybersecurity posture. This legislation would require grant recipients to have comprehensive cybersecurity plans and emphasizes significant collaboration between CISA and State and local governments. The legislation would also allow State and local governments to make investments in fraud detection technologies, identity and access management technologies and implement advanced cybersecurity frameworks like zero trust. We would also be able to invest in cloud-based security services that continuously monitor vulnerabilities of servers, networks, and physical networking devices.

Passage of the State and Local Cybersecurity Improvement Act would provide vital resources for State IT agencies, meaning my fellow CIOs and I would not have to compete against other agencies and States. Ultimately, a specific cybersecurity grant program would allow us to better assist our local government partners and address threats from well-funded nation-states and criminal actors that continue to grow in sophistication. As I mentioned earlier in my testimony, NASCIO also supports provisions within this legislation that would ensure State governments are budgeting for cybersecurity.

We also greatly appreciate the recent passage of the American Rescue Plan Act (ARP), which includes $350 billion in flexible aid to State and local governments. While we await guidance from the Department of the Treasury on allowable expenditures, I believe the ARP will create significant resources for States to invest in legacy modernization, cybersecurity improvements, and broadband expansion over the next 3 years.

CONCLUSION

When COVID–19 spread across the country last March, my fellow State CIOs and I faced enormous challenges to ensure wide-spread remote work was manageable and secure. This was made even more difficult in States that did not have a culture of remote work. Working with our private-sector partners, we adapted to a nearly universal remote environment almost overnight.

We expedited lengthy, bureaucratic acquisition processes, deployed AI-powered chatbots to assist overburdened State agencies and assisted school districts with virtual learning. We implemented numerous digital Government initiatives to improve how citizens interact with their State government websites, a crucially important project as citizens relied more than ever on State services and authoritative information sources.

CIOs also implemented COVID–19 testing websites, contact and exposure notification applications and now, vaccine websites.

In New Hampshire, we have taken numerous measures to improve the cybersecurity posture of our entire State—including with the education and health care sectors. New Hampshire recently passed legislation that mandated the establishment of "Minimum Standards for the Privacy and Security of Student and Employment Data." Through a cooperation with the State, our schools have established a Student Data Privacy Agreement, which participating districts ask vendors to sign, in order to comply with the "Minimum Standards." We've also furthered our partnership between the State CISO and the New Hampshire Chief Technical Officer Council on issues relating to cybersecurity and privacy.

On the health care front, the New Hampshire Information and Analysis Center routinely distributes cybersecurity alerts and advisories to health care entities within New Hampshire from the State and Federal Government. A recent debilitating ransomware attack on a hospital system in a neighboring State was also a real awakening for many hospital operators in New Hampshire. It helped them to understand that ransomware can have a profoundly destructive impact on their ability to operate and treat patients, as well as understand that a centralized approach to cybersecurity is superior to the more decentralized and permissive approach employed by some organizations.

In closing, as president of NASCIO, I know I speak for all my colleagues around that country that a Federally-funded cybersecurity grant program for State and local governments is long overdue. There can be no doubt that State governments need to change their behavior and begin providing consistent and dedicated funding for cybersecurity moving forward. It is my hope that the States will follow the lead of the Federal Government in this area, especially if grant programs require them to match a portion of Federal funds. I look forward to continuing to work with the Members of this subcommittee in the creation of a grant program to improve the cybersecurity posture for our States and local governments.

Ms. RICE [presiding.] Thank you for your testimony. I now recognize Mr. Krebs to summarize his statement for 5 minutes.

STATEMENT OF CHRISTOPHER C. KREBS, PRIVATE CITIZEN, FORMER DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KREBS. Chairwoman Clarke, Congresswoman Rice, Ranking Member Garbarino, Members of the subcommittee, it is my pleasure to appear before you today to discuss much-needed efforts to combat ransomware. Given my recent experience as CISA director, I remain on a bit of a personal and professional crusade to raise attention and drive toward disruptive solutions to this growing National security threat.

I would like to start with why we are here. In 2011, famed Silicon Valley innovator and entrepreneur Marc Andreessen famously penned in a *Wall Street Journal* piece that "software is eating the world." A decade later, if left unchecked, ransomware will similarly eat the world. This is not a problem that is going to go away or solve itself. The last several years alone show that cyber criminals are not only getting better, they are diversifying and they are specializing and they are getting more brazen. To put it simply, we are on the cusp of a global digital pandemic driven by greed, a vulnerable digital ecosystem, and an ever-widening criminal enterprise.

The underlying enabling factors for this cyber crime explosion are rooted in the digital dumpster fire of our seemingly pathological need to connect everything to the internet combined with how hard it is to actually secure what we have connected. Two more recent factors have thrown fuel on the already smoldering heap: The spread of cryptocurrencies that enable the transfer of funds largely outside the eyes of financial regulators and corrupt safe havens that don't mind if a little crime happens on their turf as long as it brings home some revenue, directs malicious on-line activities elsewhere, and has the added benefit of making life more difficult for strategic adversaries.

It is important to reinforce that cryptocurrency in and of itself is not a criminal enterprise nor do I currently believe eradicating or regulating it to the point of uselessness is the answer. The challenge is to appropriately intervene to avoid societal harms while fostering a marketplace for technologies like cryptocurrency where we can both lead in innovation and maintain a globally competitive edge.

We have seen some glimpses of an appetite to address the ransomware crisis with the recent announcement of the Department of Justice ransomware-focused initiative and the Department of Homeland Security's ransomware 60-day sprint. These efforts build on prior efforts from the Secret Service, FBI, CISA, and other organizations. Critically, there are also indications that the White House is considering a more strategic approach on the ransomware front soon.

But last week was perhaps the most promising development with the Ransomware Task Force releasing its report. The task force identified where the real policy and operational gaps lie. First, the need for prioritization across the National security structure. Second, greater ransomware-focused operational public-private collaboration. Third, chokepoints in the cryptocurrency payments kill

chain. Fourth, in addressing the challenges facing the cybersecurity insurance industry.

Perhaps the area with greatest need for Government investment, however, is not necessarily within the Federal Government, but, as Mr. Goulet pointed out, within our State and local partners. The idea is simple. We can reduce a tax surface across State, local, Tribal, and territorial government organizations in this country by investing in more modern systems. In doing so, we can improve citizen services for all Americans, create more tech jobs in our communities, and continue to invest in today's and tomorrow's technology innovators. It is a way to defend against today's threats while investing in a secure tomorrow.

Ultimately, whatever the administration and Congress choose to do, there is no single solution or silver bullet. No one organization alone will solve this problem. Much like confronting election security threats or disinformation more broadly, there are a range of levers that Government and industry can pull to achieve positive outcomes.

I would like to thank the committee for holding this timely hearing. I would also like to thank you for your leadership and constant enduring support of CISA. I look forward to your questions.

[The prepared statement of Mr. Krebs follows:]

PREPARED STATEMENT OF CHRISTOPHER C. KREBS

MAY 5, 2021

INTRODUCTION

Chairwoman Clark, Ranking Member Garbarino, Members of the subcommittee, it is my pleasure to appear before you today to discuss much-needed efforts to combat ransomware. My name is Christopher Krebs and I previously served as the first director of the Cybersecurity and Infrastructure Security Agency (CISA), leading CISA and its predecessor organization, the National Protection and Programs Directorate, from August 2017 until November 2020. Over the last several years, I have had the pleasure of working with many of you as Members of the primary oversight committee for CISA and have testified in front of the committee several times.

It is an honor to appear before this subcommittee to testify about the threat ransomware poses to countless organizations across this Nation. Given my recent experience as CISA director, and now as founding partner of the Krebs Stamos Group, a cybersecurity risk management consultancy, as well as the Newmark Senior Cyber Fellow at the Aspen Institute, I am continuing my commitment to improving the Nation's cybersecurity and resilience.

In 2011, famed Silicon Valley innovator and entrepreneur Marc Andreessen famously penned in a *Wall Street Journal* piece that "software is eating the world."[1] A decade later, cyber criminals in the form of ransomware gangs have come around for their piece of the action. Considered a low-dollar, on-line nuisance crime only a few short years ago, ransomware has exploded into a multi-billion-dollar global racket that threatens the delivery of the very services so critical to helping us collectively get through the COVID pandemic. To put it simply, we are on the cusp of a global pandemic of a different variety, driven by greed, an avoidably vulnerable digital ecosystem, and an ever-widening criminal enterprise.

As we have spent the last several months debating appropriate responses to Russian and Chinese cyber activities, cyber operations that most Americans will not see any direct impact, ransomware, on the other hand, has continued to affect our communities. According to the 2020 Verizon Data Breach Report, Ransomware accounts for 27 percent of malware incidents, with the highest rate of occurrence in the education, health care, and Government administration sectors.[2]

Cyber criminals have been allowed to run amok while governments have mainly watched from the sidelines, unclear on whether cyber crime is a National security-

[1] *Marc Andreessen on Why Software Is Eating the World—WSJ*.
[2] 2021 Verizon Data Breach Report, Figure 5., pg 7. Available for download here.

level threat. If there was any remaining doubt on that front, let's dispense with it now: Too many lives are at stake. We need a different approach, and that shift is needed now. We have risen to the challenge in the past and can do it again.

THE CONTEXT FOR THE RANSOMWARE EXPLOSION

The underlying enabling factors for this cyber crime explosion are rooted in the digital dumpster fire of our seemingly pathological need to connect everything to the internet combined with how hard it is to actually secure what we have connected. Two more recent factors have thrown fuel on the already smoldering heap: The spread of cryptocurrencies that enable the transfer of funds largely outside the eyes of financial regulators, and corrupt safe havens that don't mind if a little crime happens on their turf as long as it brings home some revenue, directs malicious on-line activities elsewhere, and has the added benefit of making life more difficult for strategic adversaries.

It is important to reinforce that cryptocurrency in and of itself is not a criminal enterprise, nor do I think eradicating or regulating it to the point of uselessness is the answer. Like many other transformational technology developments, cryptocurrency has likely crossed a threshold where it is here to stay. In fact, in many markets, cryptocurrency and similar financial technology developments represent a promising future for technological innovation. Therefore, the challenge is to appropriately intervene to avoid societal harms while fostering a marketplace for technologies like cryptocurrency where we can both lead in innovation and maintain a globally competitive edge.

Even if software and services were more secure, the allure of a quick buck and no real repercussions means the forward-looking prospects for ransomware actors are quite good. But we do not even have good metrics on how good the market is, as there's no real clearinghouse of authoritative sources of information on the number of victims there are. The best source in fact may be to just ask the criminals themselves (and I'm not going to take their word for it)—they'll likely offer you cyber hygiene and security advice in their response.

Ransomware crews have been propelled and professionalized by commodity malware and specialization across various hacking techniques. The sophistication of the actors is impressive—it is not just a single gang running entire operations. Different groups of criminals have developed focused capabilities or access in different aspects of the heist and collaborate as they see fit to get the job done. This allows for a commoditization of the "kill chain," creating further opportunities to elude law enforcement and dance around international financial rules and regulations.

And while these gangs have become more sophisticated, governments have been sluggish in responding in a meaningful way. As a result, victims are often left to fend for themselves, turning to specialty incident response firms that have developed a niche industry for negotiating decryption. The costs of lost productivity, disrupted operations, inefficiency in markets, and operational recovery likely far outweigh the dollars siphoned out of the world's economies and dumped into illicit activities from human trafficking to the development of weapons of mass destruction. That's right—this malware has afforded Kim Jung Un's ability to continue to expand his nuclear arsenal. How is this still only viewed as a cyber crime?

For a few years, I have been stumping for a more coordinated approach across industry and Government that can bring defenders together, break the payment chain, and put some consequences on the bad guys either directly or have their landlords do it. But much like countering disinformation (and frankly cybersecurity in general), because of the cross-cutting nature of the problem, spanning different Government agencies with different authorities, with often competing priorities and mission sets, National governments to include the United States have struggled to make meaningful progress.

CONFRONTING THE GROWING RANSOMWARE NATIONAL EMERGENCY

We have seen some glimpses of appetite to address the ransomware crisis with the recent announcement of the Department of Justice (DOJ) ransomware-focused initiative, and the Department of Homeland Security's ransomware 60-day sprint. This builds on efforts by the United States Secret Service, the Federal Bureau of Investigation (FBI), CISA, industry efforts like the National Cyber Forensics and Training Alliance, among others. Critically, there are indications that the White House is considering a more strategic approach on the ransomware front soon.

Ultimately, whatever the administration and Congress chooses to do, there is no single solution or silver bullet. No one agency alone will solve this problem. Much like confronting election security threats or disinformation more broadly, there are a range of levers that Government and industry can pull to achieve positive out-

comes. And there are past successes in operational collaboration that can be built on to ensure future success. For example, drawing on the lessons learned from the Russian efforts to interfere in the 2016 election, a coalition of agencies, including CISA, the National Security Agency (NSA), the FBI, and others, built a playbook that first prioritized effective coordination across Federal, State, and local government agencies. Second, increasing Federal support and resources to election security stakeholders to improve defenses and response. And third, engaging the adversary to learn more about their operations but also disrupt activities where possible.

The secret sauce to our election security efforts were the clear acknowledgement that multiple agencies had the ability to contribute to the ultimate outcome and we all recognized that the greater good was more important than any individual agency's "turf" concerns. The United States along with our allies need to take a new, more strategic and coordinated approach to overcoming the emerging National security emergency posed by ransomware. Similarly, the counter ransomware "triplet" includes improving cyber defenses, disrupting the criminals' business model, and increased coordinated action against ransomware gangs and their enablers. This strategy will require Government and the private sector to contribute and commit to partnering together to break the ransomware cycle.

Improving Defenses

First, we must improve defenses of our businesses and agencies across all levels of government. Ubiquitous use of multifactor authentication (MFA) for access to networks can limit credential abuse, updated and patched systems can prevent actors from exploiting known vulnerabilities, and a well-practiced incident response plan accompanied by backed up and off-line systems can enable rapid reaction and restoration. In many cases, even these straightforward steps are beyond the reach of many companies or State or local agencies. We need to rethink both our approach to technology deployment, including MFA by default, and the Federal Government should consider increasing technology upgrade grants to States and localities to retire legacy systems and join the digital transformation.

Disrupting the Ransomware Business Model

Second, we must break the business model of ransomware. Simply put, ransomware is a business, and business is good. The criminals do the crimes and their victims pay the ransom. Often it seems easier (and seemingly the right thing to do from a fiduciary duty to shareholders perspective) to pay and get the decryption key rather than rebuild the network. There are 3 problems with this logic: (1) You are doing business with a criminal and expecting them to live up to their side of the bargain. It is not unusual for the decryption key to not work. (2) There is no honor amongst thieves and no guarantee that the actor will not remain embedded in the victim's network for a return visit later, after all the victim has already painted themselves an easy mark. (3) By paying the ransom, the victim is validating the business model and essentially making a capital contribution to the criminal, allowing them to hire more developers, more customer service, and upgrade delivery infrastructure. And, most worrisome, go on to the next victim.

We must address the ransomware business model head on and disrupt the ability of victims to pay ransom. We need to prioritize countering ransomware as a Nation. That includes appropriately investing in our Government agencies and their ability to investigate, disrupt, and apprehend criminals. We need to do more to understand the ransomware economy and the various players in the market. And at the points where cryptocurrency intersects with the traditional economy, we need to take action to provide more information, more transparency, and comply with the laws that are already on the books. This includes Kiosks, Over the Counter trading desks, and cryptocurrency. Last, we don't know enough about the ransomware economy, as it operates in the shadows. We lack a clear understanding of the scale of the problem, including the number of victims of ransomware—the denominator we are trying to improve against.

There are different ways to do gain better insight into the ransomware economy, including requiring anyone paying a ransom (as a last resort, of course) to notify the Government and provide specific details. There is an alternate model, where to make a payment to an identified (in this case an officially-sanctioned organization) victims or their agents must seek a license or similar permission from the Government prior to making that payment. The Department of Treasury Office of Foreign Asset Control (OFAC) began down this track last year, declaring ransom payments to identified entities may be a violation of economic sanctions laws. Because the identity of the ransomware actor is not always obvious, the OFAC advisory may have an overall chilling effect on ransom payments.

More Aggressive Action Against Ransomware Actors

Third, we need more coordinated action against ransomware actors using the range of authorities available to Federal agencies, as well as capabilities and rights resident in the private sector. To be clear, I am not suggesting extrajudicial kinetic actions against ransomware gangs. However, other authorities available to law enforcement and military should be on the table, with great care taken not to blur the lines between the two. Traditional approaches have clearly not been sufficient to prevent the outbreak of ransomware. More aggressive and repeated disruption of malware command and control infrastructure, like the action earlier this year against Emotet, is a good start.[3] Where there are clear ties between ransomware actors and State actors or a potential imminent threat to an event or infrastructure of significance like a National election, action should be on the table. The private sector also has options available, as demonstrated by Microsoft's aggressive policing the abuse of its trademark and source code, including last fall's operation against Trickbot.[4] When coordinated and jointly conducted, private and public sector can make the internet an inhospitable place for cyber criminals.

Collective Action Against Ransomware

Last week was perhaps the most promising development in the fight against ransomware, with the Ransomware Task Force releasing its report.[5] The Task Force, a collaboration of more than 60 experts in cyber policy, software engineering, and academia, lays out a comprehensive set of recommendations that all players in the IT ecosystem can take. The report is 81 pages packed with evidence, analysis, and practical/actionable recommendations. It's clear that they've identified where the real policy and operational gaps lie: The need for prioritization across the National security structure, for greater ransomware-focused operational public-private collaboration, chokepoints in the crypto payments kill chain, and in addressing the challenges facing the cyber insurance industry.

Perhaps most importantly, the report calls for a coordinated strategy with real leadership from Government and industry. This is a critical step forward—a clear commitment to lead from the front, to ensure the various agencies and actors are working in concert. It's not just enough for the Government to coordinate itself, it needs to coordinate priorities, actions, and investments with the private sector. These actions can include taking disruptive steps against cyber criminals. Ultimately, the attack surface is not the Federal.

The RTF also calls for standing up an international coalition, something that has existed principally in law enforcement channels, and should fold in defensive teams as well as intelligence agencies. We have shown time and time again that information sharing is most effective when the people that can act on the information—regardless of whether they are in industry or in Government—actually have that information.

The RTF, importantly, calls for additional support to businesses and Government agencies preyed on by ransomware actors. This support necessarily includes boosting preventative measures, but also sets out a set of actions that everyone can take to help victims work through an attack, and only as a last resort make payments, and even in such an undesirable event, requiring reporting and tracking. Maybe then we will get good sense of how big this problem really is and more effectively build out the tools that are needed to respond on the time scales these criminals operate on. If the U.S. Treasury is expected to facilitate incident reporting, identify suspicious activity, coordinate with law enforcement, and assist private-sector victims all within the window of the extortion threat, they deserve the tools and resources they need to move with that kind of agility and speed. The same goes with the FBI and DOJ officers tasked with executing court orders to seize crypto wallets, or the team at CISA helping coordinate, respond, or work with State and Local authorities in advance to better defend their networks. Without these additional tools and resources, the criminals will continue to exploit these seams with impunity.

Last, for the RTF's recommendations to really take hold, the administration and Congress need to start putting together a legislative package to enable the additional authorities and appropriations recommended by the group. Again, there is a clear road map for cyber-related law, recently trail-blazed by the Cyberspace Solarium Commission, another group that tackled thorny cyber problems and was able to get dozens of new cyber provisions passed into law. In fact, there are a range

---

[3] *Emotet Botnet Disrupted in International Cyber Operation | OPA | Department of Justice.*

[4] *New action to combat ransomware ahead of U.S. elections—Microsoft On the Issues.*

[5] *Combating Ransomware—A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force (securityandtechnology.org).*

of recommendations that already fit well into options the Solarium is considering as it continues developing further legislative proposals.

The Ransomware Task Force should be commended for their work over the last 4 months. They showed initiative and commitment and have delivered an actionable road map for helping us get through our current digital crisis. We have tackled and overcome challenges as great as this before, we can do it again. I encourage the administration to take the recommendations on board and implement quickly, together with private industry, and I similarly encourage the Congress to consider smart legislative action.

Increasing Funding for State and Local Government Agencies

Perhaps the area with the greatest need for Government investment is not necessarily within the Federal Government, but within our State and Local partners. I recently wrote an op-ed on this subject with a former CISA-colleague, Matt Masterson.[6] The idea is simple, we can reduce attack surface across State, local, Tribal, and territorial Government organizations in this country by investing in more modern, cloud-based systems. In doing so, we can improve citizen services for all Americans, create more tech jobs in our communities, and continue to invest in today's and tomorrow's technology innovators. No, we are not going to defend our way out of the ransomware problem, but we can close out many existing vulnerabilities, and gain additional benefits along the way. It is a way to defend against today's threats, while investing in a more secure tomorrow.

As Congress considers and debates various infrastructure investment packages, I respectfully encourage consideration of cyber and technology specific funding. Everything we do these days in some way is somehow enabled by the technologies around us. Even as we have all made dramatic shifts in the way we see our friends and family, work, worship, and entertain ourselves in this new pandemic-era, the underlying infrastructure in our communities may struggle to keep up in the coming years. The difference between the haves and the have nots will be even starker, as many Government agencies will see a reduction in tax revenues due to the economic impacts of COVID.

CONCLUSION

In this era of surging ransomware, modernizing State and local IT systems is not just good Government—it is a National security imperative. Investment and support of State and local cyber infrastructure is an investment in our democracy, our judicial system, law enforcement, and the privacy and security of our citizens. Our adversaries allow cyber criminals and their own State-supported hackers to operate from their own sovereign territory, disrupting citizen services and stealing money and intellectual property from U.S. governments and businesses alike. It is time to step up and provide all partners inside and outside Government with the support and resources they need to effectively defend themselves.

I would like to thank the committee for holding this timely hearing. I would also like to thank you for your leadership and support of CISA. I look forward to your questions.

Ms. RICE. Thank you, Mr. Krebs. Our Chairwoman will be back in a few minutes, so I think what I am going to do is ask Congressman Garbarino to begin his 5 minutes of questioning.

Mr. GARBARINO. OK. Thank you very much, Congresswoman Rice.

Mr. Krebs, thank you very much. I love that we both used the silver bullet analogy. That was very good. We have similar speechwriters, I guess.

You touched about this a little in your opening, but, as you know, over the past few years there has been a robust discussion about the need for a State and local cybersecurity grant program. While no one here will disagree that an increase in funding is vitally needed, we also need to ensure that these funds are spent responsibly and in a way that meaningfully buys down risk. I know you have to have the buy-in from the State and locals, but can you talk about specifically the role CISA needs to play in providing the

[6] *Congress needs to help modernize our digital infrastructure | The Hill.*

State and local governments with the cybersecurity guidance and expertise?

Mr. KREBS. Yes, sir. Thank you for that question. I do think we share some staff perhaps, some of my former staff at least.

So, I think we should step back a little bit and think about where we are from a legislative perspective right now. There is a lot of conversation in both chambers of the Congress about infrastructure and infrastructure investments. I think that this is a great opportunity to rethink, at least strategically, about what an infrastructure investment package looks like.

Everything we do today in our communities, in our society, in our economy has some sort of connectivity to it. It has some sort of attack surface from a cybersecurity perspective. So all infrastructure investments should include a consideration for modernizing the underlying IT systems as well as security aspects of that.

So my concept is let us do a 21st Century Digital Infrastructure Investment Act that will allow State CIOs and community CIOs, like Mr. Goulet, not just buy cybersecurity technologies, but get off some of the dated legacy systems that they have that, you know, tend to have higher recurring operations and maintenance costs; that in some cases cannot be updated and are no longer supported. That was kind-of my point about it will increase citizen surfaces, it will be more resilient to attack, it will increase tech jobs in our communities, and ultimately it will plow money back into U.S. tech companies, which will keep us at the cutting edge of the technology sector.

Now, CISA can play a role in advising State and locals, in helping administer a grant program either within CISA to help dole out those grant funds or work with an existing State grant program like over at FEMA and provide that technical expertise. We have done that in the past. CISA has done that in the past with some of the State and Homeland Security grant program fundings. So, there is the expertise there, the mechanisms are there. I think the infrastructure, so to speak, for a grant program is in place at CISA as well as at FEMA. So now it is just a matter of authorizing the program and then providing sufficient funds.

Mr. GARBARINO. I thank you very much for that answer. Mr. Goulet, would you agree with what Mr. Krebs was saying or would you like to expand on any other roles that you think CISA could provide to State and local governments?

Mr. GOULET. Yes. Well, first of all, I wholeheartedly agree on the legacy system comments. The State of New Hampshire recently conducted an independent cyber risk—a comprehensive cyber risk assessment, and the findings came back overwhelmingly pointing at legacy systems where, you know, where we found vulnerabilities. In fact, we ended up shutting down some of our citizen casing systems temporarily while we mitigate those, and so that actually motivated the agency in question to, you know, to look harder and prioritize more effort at addressing that.

We are so happy with the partnership with CISA we have seen. You know, we love the collaboration and we intend to continue that and leverage it further and provide our input as well in terms of, you know, how we can work better together. So, we very much look forward to that.

Mr. GARBARINO. Great. I appreciate that. I have some other questions, but I will do a quick one because I only have 30 seconds left and it is for everybody and I think it is just a yes or no, if you can be rapid, and some of you touched on it. Should ransomware payments be made illegal? The members of the IST Task Force were conflicted on this.

Jump in whenever you want. Wow.

Mr. KREBS. This is a tough one. I am going to hedge on this. I would say the minimum—I think we should—payments should be made at a very last possible resort. If payments are made, they should in some way be either licensed or logged and reported to the Government. We, frankly, just don't have the denominator on all the victims and it is hard to really control the rest of it from there.

Mr. GARBARINO. I appreciate that. Thank you.

Chairwoman CLARKE. I thank the gentlelady from New York for stepping in momentarily on my behalf. We are all juggling hearings during this time, so I truly appreciate it.

I will now recognize myself for questions. Mr. Goulet, currently cybersecurity is a permissible use of funds awarded under the State Homeland Security Grant Program and the Urban Area Security Initiative. I was pleased to see that Secretary Mayorkas announced earlier this year that recipients would need to dedicate at least 7.5 percent of their award toward cybersecurity.

However, in your testimony, you emphasized that there is a need for a separate dedicated cybersecurity grant program. Can you elaborate on why existing grant programs are inadequate for ensuring State and local governments develop the kind of comprehensive cybersecurity improvements necessary for combatting ransomware?

Mr. Goulet, I think you have to unmute.

Mr. GOULET. You know, we applied for grants each time in New Hampshire. In fact, we have used that grant money to develop our cyber disruption plan in the State of New Hampshire that is a strong plan. But around the States, myself and my colleagues and the CISOs in the States, receive a very small percentage of the total grant funding that goes through that program. The amounts that we are able to access are not adequate to the task.

Chairwoman CLARKE. Understood. Ms. Stifel, one of the recommendations of the Ransomware Task Force is the creation of response and recovery funds. We have seen similar proposals from the Solarium Commission and in the President's budget request. What kind of entities do you believe should be eligible for assistance under these funds and under what circumstances and what kinds of expenses would be covered?

Ms. STIFEL. Thank you, Madam Chairwoman, for the question. Yes, we, as you noted, agree that these types of funds need to be established.

As far as the types of entities that could be recipients or eligible for these funds, in the first instance I would say those that we have identified previously in this conversation today, State, local, Tribal, territorial, as well as potentially organizations that are providing critical National functions. Therefore, as I know IT is currently working through identifying or has identified these essential function entities, they would also be, in our mind, an eligible recipient.

As far as types of resources that could be—these funds could be put to, we have identified and I think I agree with other panelists who said that the legacy systems are a first priority. This is particularly the case in light of what we have been through over the past 18 months—or, excuse me, 14 months with the pandemic. The decrease in taxes that are funneling to States and, therefore, even more constrained resources to put toward cybersecurity.

So, we urge that the committee—you know, appreciative of the committee in putting forward or renewing your legislation from last session. Thank you.

Chairwoman CLARKE. Thank you. General Davis, when we talk about ransomware we hear about how it is a growing crisis and we see statistics showing an increasing number of attacks with larger financial impacts and more disruption. What existing efforts have you seen that are currently working to defend against or mitigate the impacts of ransomware? Are there examples of actions that organizations are taking that are reducing risk that can serve as a model for others?

Mr. DAVIS. Thank you, Madam Chairwoman. Yes, I have a couple of thoughts about that and the fact that doing a lot on the front end, and even a little bit goes a long way, as we stated in the report.

So, first of all, I will just say basics matter. In many cases, increasing security in a few key areas could make a significant difference in an effort to prepare for attacks. Complex security software or complete network rebuilds may not be required. Implementing things that we heard up front by one of the Congressmen was implementing multifactor authentication or adopting password managers. Those kinds of things can dramatically improve an organization's security posture.

Although any organization, regardless of its security, could be a target for ransomware, improving baseline security and raising awareness among employees can go very far in protecting organizations from attack. There are some very basic human behavior-related actions that can help with the problem of phishing, which remains one of the most often used initial access methods for ransomware. So, I mean, just being suspicious of who is knocking on your digital front door and not answering it when you weren't expecting the visitor, so to speak, is a good way to look at some very basic things that can be done.

In addition, technology, although not the single answer, can provide some both emerging capabilities as well as legacy capabilities that can help improve this fight. So there is a whole array of things that I believe can be used up front in order to help prevent a lot of what we are seeing from the ransomware threat in the first place.

Chairwoman CLARKE. Thank you very much for your response, General Davis. I now recognize the gentleman from South Carolina, Mr. Norman, for 5 minutes.

Mr. NORMAN. Thank you, Madam Chairwoman, and thank all the ones that are testifying. I thank you for your time.

Mr. Krebs, I was on a bank board for a number of years and they had a cyber attack. It was like pulling teeth to get them to, I guess,

let the word out and to get help from others. They finally corrected it, but 2 questions.

How can we get—and I understand the reason, because their stock price, the name, you know, their, I guess, relationship with customers that may be threatened if it had gotten out. But how do we—in your opinion, what will we do to have them at least get the word out and get help from a lot of different factors? This is, what, a $20 billion problem.

Second, when an attack actually occurs, you know, if we have an emergency, we call 9–1–1. If you need the police, 9–9–9, you know. If you need an ambulance, you know, we know the number to call. But what should a company do, No. 1, to get the word out and get help? No. 2, you know, what do they do when they are attacked? Because they are kind-of left holding the bag and not really knowing who to go to or what expert that could solve the problem. Can you shed some light on that?

Mr. KREBS. Yes, sir. So, I think on your first question how do we get more organizations leaning forward and being more transparent about their events, I think things have perhaps gotten a little bit better in the last couple years, in part because some of the requirements for publicly-traded companies to file reports, public reports.

We are also seeing, I think, a new breed or strain of corporate executives that perhaps have been through enough events and they recognize that being forthcoming and being transparent and being straight-up with your customers or clients actually benefits you in the long run. Really the idea here is that do you want to be straight-up with your customers or do you want to hide something from them and then they go away because they don't trust you? That trust is the coin of the realm and you have really got to protect that.

So, I think in part we need to explore for at least those most critical infrastructures, as Megan Stifel mentioned, that there are some degree of—or some sort of requirements for them to make notifications at a minimum to the Federal Government and to law enforcement. But more broadly, we have to continue to reinforce with our friends in the executive community, boards of directors, that it is ultimately in their best interest to be a good corporate citizen and come forth.

On your second piece, how do we get more prepared, well, that is actually probably the most important part right now. It goes to what General Davis said about that ounce of prevention, pound of cure. You know, there is, at least in FEMA, natural disaster calculations that a dollar invested up front in mitigation saves you $4 in incident response. The same thing applies here. The cost of responding to it, even if you pay the ransom, the cost of responding to a ransomware event are massive. It is not a guarantee you get everything back. So, it is all about preparation and planning.

If you do have a bad day, because everybody has a bad day sometimes, do you know what to do? Do you know how to respond? Do you have a team on contract? Do you have relationships with CISA, with the FBI, with the intelligence community where you can get on top of this thing quickly as soon as you detect it and shut it down? So it is all about preparation and playbook planning.

Mr. NORMAN. OK. Quickly, I guess this will be for anybody, I don't want to go over my time, but regulations. OMB had a—GAO had a report that 49 to 76 percent of regulations are redundant when it comes to cybersecurity. What is your opinion on that? Again, say if it is problem, getting it cured, do you go to OMB? Who do you go to?

Mr. Krebs, we will start off with you.

Mr. KREBS. Yes, sir. So, I think we need to look at different levers we can pull here. The Federal Government has procurement powers, one of the largest procurers of, for instance, IT technologies. I think what we are probably going to see out of the White House with an Executive Order is increased and enhanced security requirements for software. That is going to have a trickle-down effect through the rest of the economy. But I still think that there are specific parts of the economy, those highest-risk, critical infrastructures, that have enjoyed an enormous amount of success in the economy and they have to step up from a corporate citizenship perspective and apply enhanced security requirements. That is an area to explore for regulation.

Mr. NORMAN. Well, I am out of time and I don't want to take other time, but help us do that. Because you all are in a position to let us know.

Thank you, Chairwoman Clarke, I yield back.

Chairwoman CLARKE. I now recognize Ms. Jackson Lee of Texas.

Ms. JACKSON LEE. Thank you very much, Madam Chair. This is Congresswoman Sheila Jackson Lee and I just want to make sure you all can hear me. Thank you to the Ranking Member for holding this hearing that is crucial and one that we have been immersed in for those of who have served on this committee for quite a long time.

To each of the witnesses, very grateful for your presentations dealing with how we deal with ransomware. I remember being a Chair of the Transportation, Security, and Infrastructure Committee, which now is now the Cybersecurity Committee, and we were talking about the amount of cyber in the private sector, which at that time was 85 percent versus 15 percent of governments. But what we really had come to find out is that we all are interrelated.

So, let me focus my questioning. As I do so, let me acknowledge former Director Krebs of CISA. We are grateful certainly for your service and regret the fact that your work as head of CISA ended over your principled stand that the election was, in fact, a legitimate election and that you had seen and determined that there was no cyber fraud or any kind of fraud under your jurisdiction that would have countered the election of Joe Biden. Principles in Government I think is crucial and I want to particularly thank you for that.

My work in the 117th Congress has included introducing H.R. 119, the Cyber Defense National Guard Act; H.R. 118, the Cyber Vulnerability Disclosure Reporting Act; and as well H.R. 57, the DHS Cybersecurity Asset Protection of Infrastructure Under Terrorist Attack Logistical Structure Act, which is called the CAPITALS Act. I hope in this Congress we will be able to pass these legislative initiatives, in particular because they really deal with the vulnerabilities of the system at this time.

I would like to pose to you, Director Krebs, because of your current past experience, if you will, dealing with this agency. What I recall is that you were very interested in standing this agency up and making it stronger. I would be interested in your understanding of the strength of the Ransomware Task Force and some of the provisions that it offered, but in the course of you saying that, I would like to know what Congress could do to strengthen this agency. I believe it should be given greater jurisdiction and support with resources. What ultimate role, how large a role do you believe the agency should play in combatting ransomware?

We always say that the large amount, as I said earlier, of this cyber infrastructure is in the private sector. I believe, however, Government can be very effective in helping to steer that sector along with their cooperation.

Director Krebs.

Mr. KREBS. Yes, ma'am. Thank you for that and thank you for the kind words. It certainly was an honor of a career and of a lifetime to serve as director of CISA. But I will say that I am incredibly excited for the agency and for the nominee for the next director, Jen Easterly. I have known her for quite some time and she is an absolute rock star and she is going to do great things there, which brings me to your question about what more can we do here, what more can we do next?

I think the last several years, particularly the National Defense Authorization Act of 2021 was very beneficial to CISA. In fact, I just read a letter or an article this morning that the agency has used its administrative subpoena authorities recently and that was something that I had asked for last Congress. It would allow the system to make notifications on vulnerable systems to IT providers. That is the sort of thing that can help.

I think ultimately the area that CISA needs the most support from Congress in that we have seen in the previous support and we need to expand from here, what I would always say is the future of CISA is in the field. So, we have now State-wide coordinators or one in or on the way to at least every State capital to work with the State CIOs, to work with the election officials. That is an area that we need to consider continuing to do. So, we need not just 47 of them, we may need 150 of them because there is plenty of work out there for everyone to do.

I also think we need to think about as we resource a grant program, what additional shared services can CISA provide? We see CISA providing shared services for the Federal Government through programs like Continuous Diagnostics and Litigation, the recently awarded Protected DNS Service, and also the hardened Cloud environment that CISA is going to provide for the Federal Government.

Can CISA build a gold image almost Cloud service that States can use, get some economies of scale, get centrally monitored and logged? Those are the sorts of game-changing technologies that I think can really help manage security better.

Ms. JACKSON LEE. Thank you so very much. Thank you, Madam Chair. Thank you very much. I yield.

Chairwoman CLARKE. The gentlelady's time has expired. The Chair recognizes for 5 minutes the gentleman—I am sorry, the gentlewoman from Tennessee, Ms. Harshbarger, for 5 minutes.

Ms. HARSHBARGER. Thank you, Chairwoman Clarke and Ranking Member Garbarino and all the witnesses. This is something really alarming. You know, when I read this report, 2,400 U.S.-based Government health care facilities and schools that were victims, that is unbelievable.

You know, when I was on another committee here, it seemed that our own Government, our Federal agencies can be hacked due to apps and upgrading or updating apps. That is a scary proposition to know that.

I guess it is just a statement and then I can go to each one of the Members. As everybody knows, the cyber incident reporting has been a significant point of interest on significant cyber incidents. The committee is interested in better understanding the right combination of mandatory incident reporting with appropriate incentives.

I guess, Mr. Krebs, I can start with you and open it up to the whole panel. Should our intelligence and law enforcement agencies be given carte blanche to take down the networks of people and organizations perpetuating ransomware?

Mr. KREBS. I think that there is always a set of trade-offs when you talk about the intelligence community and their activities. I think they are historically focused on, you know, the exquisite threats, the intelligence capabilities. But I think what we are seeing, as evidenced by recent Department of Treasury sanctions, is that ransomware gangs and foreign intelligence services are working hand-in-glove. They are in fact taking direction. Evil Corp was a Russian crew that was taking direction from the FSB. Those are the linkages that we really need to explore. That to me I think is what really kind-of tipped ransomware over into the clear National security threat. Once you have those linkages, I do think that opens up additional authorities for consideration by the Title 10 and Title 50 organizations.

Ms. HARSHBARGER. Mr. Davis.

Mr. DAVIS. Congresswoman, I agree with Chris Krebs on this. I will just tell you from the perspectives of my experience in Government, including now in the private sector, it is a blurry world out there in this murky cyber-related business between state and non-state actors. I believe that states now see an opportunity to leverage non-state entities in a variety of ways to fundamentally undermine and gain an advantage over Western democracies in general, not just the United States. This is in the area that you have covered in terms of misinformation and disinformation, but it is also in ways to circumvent sanctions. These have been through the specific capabilities associated with ransomware. We have seen various states now that have begun to embrace this idea of leveraging these other entities, criminal entities and others, in order to undermine democracy. I think that what we are seeing is this is just another reason why the task force has taken the position that you all seem to agree with, this is now a National security-related threat.

Ms. HARSHBARGER. Absolutely.

Mr. Goulet.

Mr. GOULET. Well, I think that real time, as we are—our networks are being hammered by these actors, both, you know, the nations and the nation-states, as well as other actors. So the volume of that, if it continues to increase and our relative investment on the things that we need to do there to protect ourselves needs to increase. So we are absolutely right in the middle of that swirling mass of things. I think it is partly—it has been traditional because the State governments carry a lot of information that could be useful for our enemies. Also I think that—you know, there is so much important stuff happening at the Government level, whether it is State or local. Like, for—a great example would be, you know, a computer-aided dispatch that is being shut down by a law enforcement agency, you know, where that is—you know, or dispatching for ambulance, that kind of thing, which we have seen happen. It is really a big deal.

You did mention incident reporting, which I wanted to touch on. I have legislation pending in New Hampshire that would mandate incident reporting in, you know, our political subdivisions to the State so that we can collaborate better. I have had a couple of occasions where I found out about an incident in school or a police department from the press versus from hearing about it and it is not a great way to collaborate.

So I think, you know, going on that theme that, you know, it is not shameful to have a cyber incident happen to you. In fact, it has probably happened to almost every agency and we all need to, you know, be transparent, report, and respond better.

Ms. HARSHBARGER. Absolutely.

Well, I think my time is up. I yield back. Thank you.

Chairwoman CLARKE. Thank you.

The Chair now recognizes for 5 minutes one of our preeminent experts in this space, all things cyber, the gentleman from Rhode Island, Mr. Langevin, for 5 minutes.

Mr. LANGEVIN. Very good. Thank you, Madam Chair, and thank you for organizing this important hearing today. I want to thank our witnesses for your testimony and great contribution to our efforts to try to better protect the country in cyber space and get around here on this vexing problem.

So I wanted to begin of course by congratulating General Davis and Ms. Stifel and all the co-chairs of their Ransomware Task Force for the report. I believe it is an important document and a fine example of industry self-organizing to put forth important policy recommendations.

This is an issue—cyber is something the Government can't solve on its own, private sector can't solve on its own, and it really needs to have that public-private partnership. It is great to see you acting as a resource.

So let me begin—and I also of course want to thank Former Director Krebs for being here today. I want to echo the comments of my colleague from Texas in thanking you for your—certainly your service at CISA and especially securing our elections.

But so, Mr. Krebs, in your testimony you referenced the work of the this Solarium Commission as a model for making these recommendations a reality. One of the recommendations we got done last year—no small thanks to—no small part I should say—thanks

to your help in so many in creating a Joint Cyber Planning Office at CISA. What role do you see for the JCPO in Ransomware Task Force recommendations?

Mr. KREBS. So thank you for that, and good to see you again. As we heard from the Ranking Member, you know, twice in 24 hours is a pretty good streak here.

What needs to be done within the Federal Government right now, and this is frankly one of my greatest frustrations over the last 4 years, is we needed a strategic approach to countering ransomware given the fact that there are a multitude of agencies that have an authority, a lever, or some sort of influence they have over the problem set.

So let us begin with the White House National Security Council stating that this is going to be a National security imperative to counter ransomware. So with that stage set you can declare whatever the policy is and then turn it over to an operational piece. There are a couple of operational pieces that already exist. You have the National Cyber Investigator Joint Task Force that the FBI hosts that runs campaigns, you have the National Cyber-Forensic and Training Alliance in Pittsburgh that also does some information sharing, but I think again we need to bring together the broader set of authorities from law enforcement to civil defensive agencies, civilian agencies, the IC and the Department of Defense. The JCPO could play a role there to coordinate operations.

Mr. LANGEVIN. Thank you. I appreciate the answer. I strongly support leveraging the JCPO to coordinate this kind of campaign planning in coordination with the National Cyber Director. I have been briefed several times by the Executive Assistant Director Goldstein on the stand up of the JCPO. I certainly believe it will be well-positioned to coordinate a whole-of-Government effort.

So let me turn next to Ms. Stifel and General Davis. This subcommittee focuses a lot on CISA's Federal network defense role and we have closely monitored the Federal response to SolarWinds. However, CISA has a much broader responsibility to coordinate protection of critical infrastructure that I am concerned are significantly under-resourced.

So the Cyberspace Solarium Commission has recommended increasing CISA's funding by $400 million next year to help increase operational capacity to address threats like ransomware. Do you support such an increase and do you believe it falls in line with the Task Force report?

General Davis, I want to start with you and then Ms. Stifel.

Mr. DAVIS. Sure, Congressman.

I don't know about the specifics of it from a Task Force perspective. I do know that we—that the Task Force report specifically speaks about the role of DHS in a number of different areas. I believe there are, if I have it right, 10 of the recommendations across each of the 4 main—you know, deter, disrupt, repair, and respond—functions have what we recommend is a role either as a leading role or a supporting role for DHS. So in order to do this, you know, DHS and CISA specifically have really an over-sized role and they need the support—adequate support in terms of skills, capability, capacities, and authorities.

So I would—I don't know what the right answer is, but I do believe that in order for DHS, and CISA specifically, to pick up the roles and responsibilities that we are recommending in these 10 various recommendations, it appears we are going to require commensurate resources, and that will be above and beyond what they currently have today.

Mr. LANGEVIN. Thank you. I know my time has run out, but, Ms. Stifel, do you have anything briefly?

Ms. STIFEL. I would agree with John. Thank you, Congressman, for the question. I do agree that additional resources are necessary for CISA to step into and mature into the organization that it needs to be in order to better protect the homeland.

Mr. LANGEVIN. Agreed. Thank you all. Appreciate that.

I yield back.

Chairwoman CLARKE. Thank you, Congressman.

The Chair now recognizes for 5 minutes the gentleman from Georgia, Mr. Clyde.

Mr. CLYDE. Thank you, Chairwoman Clarke, and Ranking Member Garbarino, for holding this very important hearing.

In my district, though we are mostly a rural district, we had a very detrimental attack that occurred to a local manufacturing company, called ASI. That ransomware attack completely shut them down for almost 6 weeks. Though the ransom was only $100,000 in bitcoin, it cost them over a million dollars in hard cash to replace their systems in order to recover. So this a very, very serious issue, not just for Government entities, but for commercial entities as well.

So my question goes to Mr. Krebs here. I was reading in the ransomware guide, which I thought was a pretty amazing document, that CISA offers a no-cost vulnerability scanning service and other no-cost assessments. So I followed the links in the guide to a document that further explained these no-cost cyber hygiene services, what they were, and they included vulnerability scanning, web application scanning, phishing campaign assessment, and remote penetration scanning, which I thought was very outstanding. From what I have read they are available to all agencies, Federal, State, local, Tribal, and territorial, as well as public and private-sector critical infrastructure organizations.

So 2 things here quickly, how does CISA get this guide out and get the word out on these services, which I think are phenomenal? Can you explain how an entity would sign up for them? Then how would you also determine what a critical infrastructure entity is in the private sector?

Thank you.

Mr. KREBS. Yes, sir.

So what you have highlighted here was one of my biggest concerns. There is a great deal of technical acumen and expertise at CISA, really good cyber expertise. Marketing on the other hand was never a real area of strength. That goes back to my earlier point of the future of CISA is in the field. One of the greatest ways that—the best ways to engage with our stakeholders, which are not all the time, at least in the Beltway, is to get out there and mingle in their community. As a Georgia native I know your district quite well, spent a lot of time up there playing sports and all that good

stuff. But we would need somebody that would be in that area that would be meeting with the State and local representatives, that would be meeting with the critical infrastructure. Then just from a critical infrastructure perspective, we tend to know what the riskiest stuff is out there, but a lot of it is self-selection. Again, it is marketing, marketing, marketing. It is customer-centricity, it is getting out there with constant engagement and asking what do you need.

Mr. CLYDE. OK. Great. Thank you.

The question about what determines whether an entity in the private sector is critical infrastructure or not, do you guys make that determination yourself, or is there something that you go on, a definition that you go on?

Mr. KREBS. So critical infrastructure in the United States is anything from banks to bridges, schools to sewers. It is a broad categorization that would lead an organization into a partnership, a voluntary partnership with CISA.

There are critical infrastructures that at greatest risk can be identified and tagged by CISA. There is no, you know, regulatory requirement necessarily that goes along with that, but it tends to be a self-sorting mechanism that brings organizations in to work with us.

Mr. CLYDE. OK. If any private-sector organizations choose to work with you, I assume that CISA gives them the complete confidence that any data that they share, anything that is—is held in complete confidence with CISA.

Mr. KREBS. We have a pretty good track record. Yes, sir. Or at least as I was there prior, of not sharing or leaking or disclosing information about partners. There are some regulatory protective measures, the Protected Critical Infrastructure Information Program that actually has criminal penalties on Federal employees that disclose information.

Mr. CLYDE. OK. That is great to know. Thank you.

One last question, you made a comment about chokepoints across the cryptocurrency. Because I think cryptocurrency, you know, it is a common denominator in all ransomware, because that's how they get paid.

So can you talk a little bit about chokepoints? How we can improve chokepoints maybe and make cryptocurrency harder for people to use anonymously?

Mr. KREBS. Well, so I think the way I would characterize it is you have the up points of leverage where the cryptocurrency economy intersects with the conventional economy. It is in kiosks, it is over the counter desks, it is exchanges. Any time that you are taking bitcoin, you are buying bitcoin, or trading it out, those are areas that you can actually say, look, you have to comply with financial regulations, know your customer, anti-money laundering. The Task Force does a fantastic job of laying out some of those issues.

The thing that we have to be careful about is cryptocurrency is one of those technologies that has crossed the threshold in my view. It is here to stay. In fact, there are other emerging—you know, in China cryptocurrency is way, way, way ahead of where we are in the United States. If they are likely—it is going to be, you

know, the future of financial transactions. So rather than cut it off and strangle it, we need to figure out how to get the outcomes we want, positive societal outcomes, while reducing and minimizing. I think that is the area that Congress needs to spend a lot of time policy-wise thinking about.

Mr. CLYDE. Thank you very much.

Chairwoman CLARKE. The gentleman's time has expired. Thank you. Thank you for your questions, Mr. Clyde.

The Chair now recognizes for 5 minutes the gentlewoman from New York, Ms. Rice.

Ms. RICE. Thank you so much, Madam Chair.

I do hope that we take the recommendations that the Ransomware Task Force made and incorporate it into some kind of legislation as quickly as possible because what I am hearing from both sides of the aisle during this hearing is that the recommendations are good, especially, you know, making the United States lead by example and execute a sustained, aggressive, whole-of-Government, intelligence-driven, anti-ransomware campaign that is coordinated by the White House in the 4 ways they—or the 3 ways that they mentioned because that is critical. We have to have one mission, we have to have a specific way to execute that.

Mr. Krebs, just a couple of questions that I would like to direct to you. There were 560 ransomware attacks on U.S. health care facilities in 2020 in the middle of this pandemic. I am sure that you would qualify health care facilities as critical infrastructure. I would just like to get your opinion on what we can do to ensure—and, by the way, the pandemic I think made clear that there is a fundamental connection between strong public health infrastructure and strong National security. So I want, you know, your thoughts on that.

In my district in 2019 as part of an attack that targeted several school districts around Long Island and New York, 2 school districts in my district were targeted by cyber criminals and had all of their data held for ransom. One district had all of its data backed up off-line and didn't need to make the ransom payment to the attackers, but unfortunately the other was forced to pay nearly $100,000 to regain access to its data.

I guess they would be going back to do you criminalize the payment of ransomware, but also is there best practices that say school districts—like one of them knew to keep this stuff off-line, the other did not and had to make the payment. What are your thoughts on that?

Also I just really wanted to get into the cryptocurrency issue again. I mean we have been talking about this—in all my years on Homeland Security, talking about cryptocurrency and the use of cryptocurrency by terrorists, but now it is becoming much more accepted and daily used form of payment for not just terrorists, but here we are with ransomware and, as you say, every day in China and it is going to become much more ubiquitous.

So your thoughts on that as well.

Mr. KREBS. OK. So, OK, there is bitcoin, there are schools, and there are hospitals. On the hospitals point, in the middle of COVID, your number 560, that is at least what we know. One of the biggest problems we have right now in cyber crime and

ransomware specifically is we don't actually know—we don't have confidence and granularity on the actual denominator because there is a lot of lack of reporting. So we need to work through how do we get a better fidelity on the numbers of actual victims. So the Ransomware Task Force had some recommendations on requirements for paying for ransom. Because, you know, school setting is an opportunity is for CISA and the Department of Education, both at the Federal and the individual State levels, to work together to develop best practice and guidance. I think that is under way over the last several months to pull that together.

Last, happy to come in and bring some experts in to talk about Bitcoin, but this is—or cryptocurrency, rather, more broadly. Again, we need to think about, you know, boosting innovation and reducing the harms.

Last point I want to make here though is that based on my experience in leading CISA, the budget process and the appropriations process is critically important on seeking the outcomes that you want as Congress. When you dedicate specific resources sufficiently to tackle a problem, for instance election security, then that allows us to put surge resources to that problem. So if ransomware is a priority, then you need to think about what is it going to take from a unit type cost perspective to achieve the outcomes you want so that there can be hiring, there can be certainty in contracting, there can be other resources acquired and brought in.

I am telling you right now, the approach we took to election security is but one of the critical infrastructure sectors. In fact, 1 of 55 National critical functions. It required a significant amount of focus and personnel and resources, but it can be repeated. We can repeat that same model to counter ransomware. But, again, you can't just say, hey, you guys have to do this now out of your existing budget. We have to put resources against it and it will get done. I promise you that.

Ms. RICE. Well, I couldn't agree with you more.

I want to thank all of the witnesses here today because with a brain trust like you helping legislators like us, I don't know how we can't get this done. We just have to get behind it in a nonpartisan way and get the job done.

Madam Chairman, I yield back. Thank you so much.

Chairwoman CLARKE. I thank the gentlelady.

Let me just address an issue to remind Members that pursuant to House rules Members are required to be on camera when recognized during committee proceedings. Members may be allowed to participate without video where they are having technical difficulties.

Having said that, I would like to now recognize for 5 minutes the gentleman from New York, Mr. Torres, for 5 minutes.

Also inform colleagues that we will likely have a second round of questions for our witnesses, so those of you who may have additional questions, there will be a second round following Mr. Torres.

Mr. Torres, the floor is yours.

Mr. TORRES. Thank you, Madam Chair.

According to Cybersecurity Ventures, the cost of cyber crime has been on an exponential curve, with $3 trillion in 2015 to a projected $6 trillion in 2021, to a projected $10.5 trillion in 2025. Ac-

cording to Third Way, almost all cyber crime goes unpunished with less than 1 percent resulting in enforcement action.

My first question concerns prevention and it is directed toward Mr. Krebs. In your professional judgment, would protective DNS services be effective at preventing most ransomware breaches?

Mr. KREBS. Most ransomware breaches, I think that is hard to say. I think it would certainly be an effective way to detect malware on a network. And help minimize any sort of further compromise.

Mr. TORRES. What about the efficacy of multifactor authentication?

Mr. KREBS. Well, that is just—that is table stakes. This is one of the biggest problems right now that we are seeing I think in State and local communities—and I would love to hear Mr. Goulet's perspective—but some of these State and local organizations, Tribal and territorial as well, don't have the resources to shift off of some of their legacy systems and don't have the staff to implement a multifactor authentication regime. They rely on single-factor authentication, like passwords that are easily brute force, password sprayed, and things like that. I think we need to give them the resources to make that shift, but we also need to put additional pressure on some of the technology companies that are providing the services and say, look, MFA, multi-factor authentication, by default has to be the new normal.

Mr. TORRES. A quick question about reporting. If a Federal contractor were to make a ransom payment using Federal funds, would the contractor be required to report the incident to the Federal Government?

Mr. KREBS. I am not clear right now on some of the Federal acquisition regulation requirements on that. But I mean if it is not, it certainly should.

Mr. TORRES. You know, it seems to me that the scandal is not only that we are failing but in many ways we are not even trying. Most State and local governments have no separate line item for cybersecurity, which tends to be buried in the larger IT budget. My understanding is that State and local government on average dedicate only 1 to 3 percent of their IT budget on cybersecurity.

In your estimation, what percentage of a State or local government's IT budget should go toward cybersecurity?

Mr. KREBS. Percentages of overall IT spend dedicated to cybersecurity is a metric that sometimes gets thrown around as a good way to measure. I don't think it is always that helpful because you could spend 15 percent of your budget on stuff that doesn't do anything for you. So it is about are you investing in the right things, like multifactor authentication. I think for State and local, I think getting to the cloud, you know, getting off of your on premises exchange servers, segmentation of your networks, recovery, incident response planning and exercises. I think those are 4 or 5 of the things that I would put a lot of focus on.

Mr. TORRES. I know the Task Force on Ransomware has put forward 48 recommendations. I suspect many of those recommendations are familiar proposals that have percolating for a long time. I am curious now what historically has been the greatest barriers to the implementation of those recommendations and what can be

done to break down those barriers. This question is for both General Davis and Megan Stifel.

Mr. DAVIS. Thank you, Congressman. I will go first while Megan is considering her response.

There are a lot of good things that are out there that exist today. I think part of the problem though is that, No. 1, I was in the prepare working group. I was a co-chair in that working group as well. What we came to the conclusion was that for a variety of reasons organizations, especially the smaller ones, both in the public and the private sector, were either unaware of or there was a failure to adopt it for a number of reasons. That is why one of the—in my opinion, one of the biggest recommendations that we made was to come up with this framework, this internationally-accepted, accessible, practical framework of the best practices that exist out there today so that this information can be made available.

In terms of adoption, part of the challenge with adoption was the aspect of—especially at a smaller organizational level, when you only have so many dollars, it seems that most of the business decision making is done concerning availability when it comes to information systems and not security.

So part of the recommendations we made was also to get after that audience of business decision makers to arm them with the information that would enable them to make better risk management decisions within the context of the business and not simply IT decisions.

Then just from the general perspective, I think a lot of the reasons why some of the good things that are out there just aren't adopted as wide-spread as they could be is the fact that it has been stovepipe and piecemeal, and there is a lot of noise that needs to be sifted through.

So I think our approach is this full court press with, you know, all of these required participants in order to solve some of those challenges.

Ms. STIFEL. I am happy to respond. The time has expired, but I would agree——

Chairwoman CLARKE. Yes, the gentleman's time has expired and we are going to enter into a second round of questioning. So I just wanted to—if you can just hold your comments and you can probably tack it on a response to some additional questions.

I now recognize myself for the beginning of the second round of questioning.

My next question goes to General Davis and you, Ms. Stifel. The Ransomware Task Force report observes that there is a lack of reliabile representative data about ransomware scope and scale. DHS has long worked to incentivize cyber information sharing with somewhat mixed results.

How can the Federal Government best incentivize State, local, and private-sector entities to share timely, actionable information about ransomware incidents?

Mr. DAVIS. Madam Chairwoman, I will be brief since I hogged the last question and didn't give Megan a chance to answer.

But I will just say that from the perspective of the Task Force, information sharing—threat intelligence sharing and information sharing was seen as absolutely critical and that there is a lot of

good work that has been done, especially with the Cybersecurity Information Sharing Act of 2015. All we are recommending is that that be reviewed with an eye toward ransomware specifically. There are some new indicators of compromised and contextual information specifically around ransomware that we believe can be integrated into the existing regimes to make improvements where required.

Chairwoman CLARKE. Ms. Stifel, your impressions? I know you wanted to jump onto the last question.

Ms. STIFEL. So first I would say with respect to information sharing, agree with John that a great deal of work has gone into and been successful in enhancing that capacity over the past 5 years. Still I think there is an opportunity for enhanced awareness around the importance of this information, especially as it relates to ransomware, but also of the incentives, so to speak, that are offered to entities that do share information with the Government. I think there are still, you know, hesitance and that can be reduced through a range of opportunities, including valued members of the panel with me in highlighting the value of sharing information.

On the last piece, I think part of the challenge relates to knowing that there is a strategy. Improving the ability, again, to highlighting the real threat that ransomware has become and ensuring that the available resources that exist are known to entities that meet them when they need to respond to them, as well as to help better prepare them.

Chairwoman CLARKE. Very well. Thank you for your response.

Mr. Goulet, the COVID–19 pandemic highlighted how dependent we are on technology across Government and business. In particular, we saw how under investment in State IT budgets strained the ability of Americans to access certain programs, such as enhanced employment benefits.

How has the pandemic affected States' risk to ransomware and how could a ransomware attack impact a State's ability to distribute Federal benefits to residents?

Mr. GOULET. Well, thank you.

Well, with the, what I call the Diaspora, with all the people, you know, moving home to work early last year, where the attack surfaces for any cyber attack just massively increased because of, you know, where basically people's home networks became part of our State networks as part of that. Really the criticality of these systems became so much more important, particularly like our unemployment systems or our case management systems, where we use them for contact tracing and vaccinations.

So, you know, the extra effort and impact of—we can imagine—in fact we had sent out a special to all employees in New Hampshire early in COVID saying don't be the one that clicks on a link and takes down our unemployment system.

I would also have to comment on the multi-factor authentication that came up earlier. Many States are implementing that. It is a financial challenge for many States, but it is absolutely critical, especially for systems that are—where administrative access such—those with administrative access accounts. It is absolutely critical that multi-factor authentication be implemented.

Chairwoman CLARKE. Very well. Thank you very much.

Ms. Stifel, you mentioned in your testimony that 70 percent of ransomware attacks in the fourth quarter of 2020 involved the threat to release data, in what some call double extortion ransomware. That is a startling change from the traditional ransomware practice of just denying access to data or networks.

What do you think is driving this change, how does this additional threat shape victim's behavior, such as their willingness to pay a ransom, and how have these threats increased the impact that ransomware has on victim organizations?

Ms. STIFEL. Thank you, Madam Chairwoman. That is a great question.

I would say there are a number of factors that are influencing this shift. The first is that in some cases—I think it was in about 20 percent of cases—ransom payments were being made, and so the need to—and the fear that private information, particularly if it is intellectual property, might be hacked and dumped on-line can—incentivized criminals to try and take this approach thinking that they are more likely to get paid.

Similarly, the fact that in many cases now organizations have back-ups—may not be fully comprehensive, but we heard story earlier in this hearing about one school system being able to restart from back-ups and the other not. That can also frustrate criminals and so they need to pivot to an alternative business model to try to continue to fund their malicious activities.

The third I think is really that the ability for criminals to—where victims are not making clear that they have been the victim of an incident, by dumping the information they are demonstrating their prowess, so to speak. So really I think one of the things that people need to think about as they are working to mitigate and prevent these types of activities is, again, the utility of encryption and encrypting data at test and in transit so that where files were—an actor gains access to the network, they are still limited in their ability to gain access to these essential files.

Chairwoman CLARKE. I thank you.

I have gone over time, so let me now recognize the Ranking Member of the subcommittee, the gentleman from New York, Mr. Garbarino, for his questions.

Mr. GARBARINO. Thank you, Chairwoman, for the second round. I appreciate it.

Quickly, Ms. Stifel. You mentioned many CRRFs in your opening statement, Cyber Response and Recovery Funds, yet the ransomware report states that only about one-third of affected companies pay the ransom. What would prevent a company that was never planning to pay the ransom from applying for free money from the Government to rebuild. Does this effectively take away the incentive for private sector to modernize and securitize their systems if they know the Government will pick up the tab? Should there be some sort of cost-sharing arrangement in your opinion?

Ms. STIFEL. Thank you, Congressman.

Yes, the Task Force recommends that not just a blank check so to speak be offered to entities that are applying to receive assistance through the Cyber Response and Recovery Funds, but in fact there being some set of criteria after which they might be able to access the funds.

So in the case of the Task Force, the example was one a framework is developed that identifies practices that could be undertaken to better prevent ransomware victimization in the first place, demonstration of compliance with or the ability to meet the suggestions and the framework be one doorway through which an organization might access the funds.

Mr. GARBARINO. Thank you very much.

This is both for General Davis and Ms. Stifel. You both participate, you are both co-chairs of the Task Force. I believe one of the priority recommendations advocates to know your customer. Another requirement is on cryptocurrency exchanges. Can each of you expand on that recommendation? If there is time, Mr. Krebs, maybe you want to jump in as well.

Mr. DAVIS. Thank you, Congressman. I will go ahead and start.

But obviously the recommendation is that what we found from the Task Force perspective was that ransomware crimes should be more closely regulated and Government should require cryptocurrency exchanges with crypto kiosks, the over-the-counter trading desk, to comply with existing laws. Those were the ones including know your customer, anti-money laundering, and combatting the financing of terrorism. In our view, those are good laws, they are just not effectively and consistently implemented in all cases. Great oversight and the ability to enforce those we believe would actually put a dent in this problem.

Ms. STIFEL. Just a little bit on what John said to you highlights the importance of the information that can be gathered through these types of requirements. Those cannot only facilitate the investigation of the crime itself, but also it is preventative measures that law enforcement and others can take in trying to again deter the number of ransomware attacks.

Mr. GARBARINO. Mr. Krebs, is there anything additional?

Mr. KREBS. I think that covers the fair share of it. Again, I think what we have to focus on is increased—and I can't believe I am saying this right now—but increase the information sharing on victim—not personal information, but victim wallets to the extent that we can get better fidelity on the size and scope of this issue and where the funds are going to light up those aggregation points throughout the economy, the cryptocurrency economy, that allows us to take further directive action against the criminals.

Mr. GARBARINO. I appreciate that. Thank you very much all.

One just final question for anyone. Are you aware of companies doing the right thing? You know, having back-ups, doing what I explained before, but it being more expensive to do the right thing than actually paying the ransom? Anybody have any stories on that?

Mr. KREBS. So I—you know, just out of personal experience, at least in the last several months, we have had a number of conversations with companies that have ultimately decided they could either rebuild or recover ultimately, somehow not have to pay. The reasons for that are going to vary from not wanting to contribute and otherwise.

Mr. GARBARINO. OK. Since nobody else has anything else to add, I yield back.

Thank you, Chairwoman.

Chairwoman CLARKE. I thank the Ranking Member.

The Chair now recognizes for 5 minutes the gentlelady from Texas, Ms. Jackson Lee. Ms. Jackson Lee, are you with us? Ms. Jackson Lee?

Well, it appears that she is indisposed. You all have been wonderful and giving of your time today——

Mr. LANGEVIN. Madam Chair? It is Jim Langevin. If it is possible to——

Chairwoman CLARKE. Oh, absolutely. I am sorry, I am sorry.

The gentleman from Rhode Island is recognized now for 5 minutes, Mr. Langevin.

Mr. LANGEVIN. Thank you, Madam Chair. I appreciate again you holding this hearing and the time and the testimony of our witnesses.

So let me go to Ms. Stifel. In your testimony and in the Task Force report, you referenced the importance of the FBI cyber assistant legal attachés, or ALATs. The Solarium Commission, on which I served, also recommended substantially increasing these positions to help coordinate international cyber criminal investigations. Can you elaborate on why these positions are so important from your perspective?

Ms. STIFEL. Thank you, Congressman. As an alum of the Department of Justice, I particularly appreciate the question.

So the ALATs are really the eyes and ears of the law enforcement community overseas and they work very closely with their host country counterparts.

So in the first instance they are there to help facilitate investigations of criminal activity that has occurred against U.S. citizens, but they are also there too as an extension of our policy approach to law enforcement activity, including our support for the Budapest Convention, otherwise known as the Cybercrime Convention. So they are there not only collecting evidence, also training local host country staff, but further extending the policy approach of ensuring that there are administrative, as well as substantive laws on the books that criminalize malicious activity and unauthorized access to computer networks and the ability to bring these perpetrators to justice. So in some cases they need to be working through mutual legal assistance activities necessary in order to further an investigation.

Of course they are also providing assistance potentially from the U.S. side where U.S. companies may be involved in host nation's investigation of an activity.

But I think it is also crucial to note that we don't have as many of these as probably could be most effective for—particularly for purposes of combatting ransomware. So I would encourage additional support for ALATs as the Solarium Commission has also recommended.

Thank you for the question.

Mr. LANGEVIN. You bet. I like how you phrased that there, they are the eyes and ears of law enforcement on the international front, if I heard that right. You know, I couldn't agree more. Right now I think there are too few of them and we really need to have more. So thank you for that.

I think there are only—people may be surprised to know I think there are only 12 of them right now; 12 is not enough and we need more.

Let me go back to General Davis, if you could. We talked in the past about the preparation of crime as a service. Very disturbing to me, certainly as it is to others, when you look at the ransomware ecosystem and business model, what do you view as the critical function with the disruption of which would cause maximum pressure on the criminals?

Mr. DAVIS. Thank you, Congressman Langevin.

First of all, I would say that once again this is a full court press and that happens to be one of the pressure points. In looking more deeply at that pressure point, I know the Task Force investigated the ability to disrupt the payment process, and it was seen as a critical chokepoint, the infrastructure associated with the ransomware model and the threat actors themselves. I think it takes all 3 of those. There are specific recommendations along the line of each of those 3 aspects of putting pressure on the act itself, the criminal enterprise.

I do think that in the notion of going after the infrastructure, there is an enormous role that private industry can play and has proven to be able to play in certain instances that are very current, for example. So I think this notion of a National-level Joint Ransomware Task Force, that involves, you know, White House-led effort with the appropriate inter-agency and the new National Cyber Director in coordination with existing organization, like NCIJTF and the JCPO, that is very important. But to get after some of these infrastructure-related disruptions, you are going to need to leverage the hub, the private industry hub, that we have also made as a recommendation as a part of that overall whole-of-society effort.

Mr. LANGEVIN. Thank you, General.

Mr. Krebs and Ms. Stifel, the Task Force recommends developing target lists of ransomware developers and other linchpins of the business model. Are there reasons the Government doing this already? Or ways that we could help it more effective?

Mr. KREBS. So I will try to keep this short, but, look, the intelligence community, law enforcement community have, just like everybody else, a limited set of resources and then a separate set of priorities that they have to work against. So I think what is needed here is let us elevate ransomware and ransomware as a service in the priority list. Now, something is going to get bumped down unless we give them more people and more money to get through this. But I do think that there is a realization in the IC that ransomware sponsored by countries like Russia is a priority. We were able to prioritize counter ransomware at least from an elections perspective. I think there is a broader effort we can do here.

Mr. LANGEVIN. Thank you.

Ms. Stifel, anything?

Ms. STIFEL. No, I agree with Chris Krebs.

Mr. LANGEVIN. OK. Very good.

I see my time is expired. Madam Chair, thank you for the indulgence and I yield back.

Thanks to our witnesses.

Chairwoman CLARKE. With that, I do thank our witnesses as well, General Davis, Ms. Stifel, Mr. Krebs, and Mr. Goulet, for your forthright answers today and as well as your indulgence in our second round of questioning. I thank our Members for their questions.

The Members of the subcommittee may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

Without objection, the committee record shall be kept open for 10 days.

Hearing no further business, the subcommittee stand adjourned.

[Whereupon, at 4:22 p.m., the subcommittee was adjourned.]

○