A WHOLE-OF-GOVERNMENT APPROACH TO COMBATTING RANSOMWARE: EXAMINING DHS'S ROLE

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

AND THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

NOVEMBER 17, 2021

Serial No. 117–38

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

47–150 PDF WASHINGTON : 2022

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 INTELLIGENCE AND COUNTERTERRORISM

ELISSA SLOTKIN, Michigan, *Chairwoman*

SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
ERIC SWALWELL, California
JOSH GOTTHEIMER, New Jersey
TOM MALINOWSKI, New Jersey
BENNIE G. THOMPSON, Mississippi *(ex officio)*
AUGUST PFLUGER, Texas, *Ranking Member*
MICHAEL GUEST, Mississippi
JEFFERSON VAN DREW, New Jersey
JAKE LATURNER, Kansas
PETER MEIJER, Michigan
JOHN KATKO, New York *(ex officio)*

BRITTANY CARR, *Subcommittee Staff Director*
ADRIENNE SPERO, *Minority Subcommittee Staff Director*
JOY ZIEH, *Subcommittee 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

A WHOLE-OF-GOVERNMENT APPROACH TO COMBATTING RANSOMWARE: EXAMINING DHS'S ROLE

Wednesday, November 17, 2021

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

The subcommittees met, pursuant to notice, at 10 a.m., at 310 Cannon House Office Building, Hon. Elissa Slotkin [Chairwoman of the Subcommittee on Intelligence and Counterterrorism] presiding.

Present from the Subcommittee on Intelligence and Counterterrorism: Representatives Slotkin, Jackson Lee, Langevin, Torres, Malinowski, Pfluger, Guest, Van Drew, LaTurner, and Meijer.

Present from the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation: Representatives Clarke, Slotkin, Jackson Lee, Langevin, Torres, Garbarino, and LaTurner.

Also present: Representatives Thompson, and Katko.

Chairwoman SLOTKIN. Good morning, everyone. The Subcommittee on Counterterrorism and on Cybersecurity, Infrastructure, Protection, and Innovation will be in order. Subcommittees are meeting today on "A Whole-of-Government Approach to Combatting Ransomware: Examining DHS's Role." Without objection, the Chair is authorized to declare the subcommittees in recess at any point. This morning, I would like to thank our witnesses from the Department of Homeland Security for joining us today to discuss DHS's role in our efforts to combat ransomware. I also want to recognize Chairwoman Clarke, Ranking Members Pfluger and Garbarino, as well as Chairman Thompson and Ranking Member Katko, who I believe are on or coming on.

In the spirit of getting to the meat of the conversation, I am going to encourage my fellow Members of Congress to shorten their opening statements so that we can get right to it. I appreciate your flexibility for our witnesses on knowing that we have many, many hearings going on right now. Many folks including Chairwoman Clarke in and out of an important mark-up. So, we appreciate your understanding.

I will just say that I think ransomware is one of those rare National security issues where you can have high-level policy debate in Washington that directly connects to the tangible impacts on

people's lives back home in places like Michigan and in Texas. We know that ransomware attacks have exploded in the United States and during a year-and-a-half where we have been more dependent than ever on digital technology, it has really hit home for certainly most of the citizens that I represent.

These attacks are overwhelmingly carried out by foreign groups. So, that means our constituents are victims of foreign attack. Ordinarily, it would not be average Americans who are, you know, receiving a foreign attack. It would be soldiers and tanks and planes who signed up to be on the front lines, not the average citizen. Colonial Pipeline and JBS Foods were certainly attacks that hit home very deeply. I would just note that our schools, our K through 12 schools, are the places where I have been hearing constant concern from our superintendents because they have been particularly hard-hit. I think we have 43 school districts in Michigan that have been hit by ransomware attacks. Obviously, deeply disruptive on top of a very disruptive year.

We know that Michigan State University, I represent, our universities have been paying ransoms to get back the data of the personal information affecting over 9,000 students. So, it is not going away anytime soon. We know that it is extremely profitable and we know that Secretary Mayorkas and Director Wray and countless others have made this a National security priority.

I think what is important to us and important to expose for the American people is what are we doing about it? Please help our citizens understand and help the committee understand what DHS is doing to fight back with our citizens on the front lines. I am pleased that we are strengthening what we are doing against ransomware. I am glad that it is bipartisan. That is an extremely important thing. We know that DHS is a key Federal player in this whole conversation, particularly given your specific role of engaging with State and locals down in our States.

People want to know where they go when they call 9–1–1, when they have got a ransomware attack. It is happening in their school. It is happening in their business. It is happening to their local government. Who do they call and how do they take care of it?

[The statement of Chairwoman Slotkin follows:]

STATEMENT OF CHAIRWOMAN ELISSA SLOTKIN

NOVEMBER 17, 2021

The threat of ransomware attacks is one of those rare National security issues where the high-level policy debate here in DC very directly connects to the tangible impact it's having on families back home in our districts, every day. Ransomware attacks against the United States have exploded in number and cost over the last few years, especially during the COVID–19 pandemic.

During a year when we've been more reliant on digital technology than ever, ransomware has disrupted half the fuel supply for the East Coast, and the world's largest meat processor—in addition to countless attacks on our hospitals, schools, police departments, and businesses. These attacks are overwhelmingly carried out by foreign groups, but their victims are our constituents. Ordinary Americans, not soldiers in tanks and planes, are on the front lines of this threat.

After the attacks on the Colonial Pipeline and JBS Foods, I'd find myself in rural communities in my district, talking about agriculture or education—and everyone from farmers to school superintendents would come up and ask me about what we were doing to protect them from this onslaught of attacks.

We're seeing the impact of ransomware all over Michigan. During the peak of the pandemic last fall, a Nation-wide attack affected hospitals in St. Johns and Auburn

Hills. And our schools have been hit particularly hard. Our State's leading insurer of K–12 schools told me that they've worked with 43 Michigan school districts that have been hit by ransomware attacks, just since the start of 2019, and paid out millions of dollars in claims.

Earlier this month, K–12 superintendents from across Michigan told me that the ransomware risks they face have become so severe that, according to insurers, their schools may be uninsurable by the end of this school year. These attacks can be incredibly disruptive for schools: Last summer, a ransomware attack on a single department at Michigan State University, which I represent, cost the university over a million dollars to recover from. The attack knocked labs and networks off-line for months and caused the loss of over a year's worth of research data—forcing some researchers to start over from scratch. And when MSU refused to pay a $6 million ransom, the attackers leaked personal information affecting over 9,000 students.

I know all my colleagues on this committee have heard similar stories from their communities.

The ransomware threat isn't going away anytime soon. Over the last 5 years, we've seen the illicit infrastructure that enables ransomware attacks metastasize, and evolve into a new business model—"ransomware as a service." Under this new model, which enabled the attack on Michigan State University, criminals no longer need the technical skills to build ransomware themselves—they just agree to pay the ransomware developer a licensing fee, or a cut of the ransom.

As a result, ransomware has become an incredibly profitable business for international cyber criminals: Between 2017 and 2020, we saw ransom payments increase from around $37 million annually, to over $406 million per year. Taxpayers and business owners, including the Michiganders I represent, end up paying those bills. As Secretary Mayorkas, Director Wray, and countless others have made clear, ransomware is a direct threat to our National security.

I was pleased to see the President lay down a marker with Vladimir Putin, in June: That we hold Russia responsible for stopping ransomware attacks coming out of its territory—regardless of who's conducting them—against the 16 U.S. critical infrastructure sectors. I'm also pleased that the Federal Government is taking aggressive steps to combat these attacks and bring cyber criminals to justice. The administration has required stronger cybersecurity across Federal agencies and vendors; given ransomware investigations similar priority to terrorism investigations; and engaged more than 30 countries to combat international cyber crime. And earlier this year, President Biden appointed the first National cyber director, to quarterback the Federal response.

These efforts to go after attackers are starting to pay off: Just last week, the Department of Justice announced the indictment and arrest of a Ukrainian national charged with deploying ransomware to attack U.S. businesses and Government entities—as well as the recovery of over $6 million worth of ransom money. I'm also pleased that taking on the ransomware threat and strengthening our cybersecurity is still a largely bipartisan cause. On Monday, I was proud to join President Biden as he signed the bipartisan infrastructure bill into law—including a billion dollars in cybersecurity preparedness grants for State, local, Tribal, and territorial governments.

I want to recognize my committee partner, Chairwoman Clarke, for leading that provision—and I thank her for working with me to include language that will help innovative local cybersecurity partnerships, like the ones we have in Michigan, benefit from this transformative investment. For its part, the Department of Homeland Security has been a key player in Federal cybersecurity efforts and is at the center of the country's counter-ransomware efforts. We are fortunate to have witnesses before us today who can speak to DHS's contribution to this whole-of-Government fight against ransomware.

I'm particularly interested in hearing about how the threat landscape has evolved—as well as how DHS is using its technical expertise, law enforcement and intelligence capabilities, and its industry and international partnerships, to take on this threat. I also look forward to discussing how DHS can help ensure that our local communities can access the resources they need, as quickly and easily as possible.

This year has made clear that cybersecurity isn't just a tech issue—it's at the heart of protecting our daily lives. I look forward to today's discussion on how DHS is leading that effort.

Chairwoman SLOTKIN. With that, I will recognize my partner on the Intelligence and Counterterrorism Subcommittee, the gen-

tleman from Texas, Representative Pfluger, please, for an opening statement.

Mr. PFLUGER. Thank you, Chairwoman Slotkin and Chairwoman Clarke, and also my Ranking Member colleague Garbarino for holding this subcommittee hearing today, which I agree with everything that was said that this is such an important time in this country to identify the issues, to come up with solutions, and to move forward. I would like to thank our witnesses for joining us today as well. This impacts every place in America, including my constituents who have recently been victims of these types of attacks. The United States right now, I think, faces an overwhelming threat from cyber crime, especially ransomware. The attacks we have witnessed over the past year on the country's critical infrastructure put the livelihood, privacy, and our way of life, the way of life of everyday Americans at risk.

The criminals behind these attacks are emboldened not only by the large sums that they command for the ransoms, but also the relative anonymity that they are able to maintain. Groups like Hafnium, Nobelium, REvil. Those groups launched their attacks from safe havens in Russia and China. They operate because of the blind eye and even encouragement that these countries offer.

I was glad to see the Department of Justice's recent indictment of two foreign nationals charged with deploying REvil ransomware to attack businesses and Government entities in the United States. I look forward to hearing about the role that DHS played in that investigation as well. Arrests like these should serve as a warning to every cyber criminal that the United States will bring them to justice no matter where they are located.

I, like my colleagues on this committee, am keenly interested in the preventative measures that American private and public sectors should be taking to mitigate these nefarious efforts of cyber criminals. From local school systems to pipelines that supply vital energy to our country. Across the country, these criminals have highlighted that everyone using modern technology is at risk. We must all take measures to safeguard ourselves and our businesses. However, when these measures fail, it is up to members of our law enforcement and our legal communities to pursue and prosecute those responsible.

When a cyber attack occurs, every minute counts. Time is of the essence and criminal investigators, network security experts, must work hand-in-glove to understand the technologies these criminals are using as well as the specific vulnerabilities they are exploiting. As demonstrated by the panel before us, DHS has several components dedicated to combatting cyber crime. I am looking forward to hearing about the many ways that these components and offices work within the Department, as well as with other agencies to combat this threat.

DHS is doing an incredible job and I commend them for their continued efforts. However, cyber criminals continue growing and evolving and we must do the same to fully protect our own cyber networks. It is important for us to understand how law enforcement entities within DHS and across the spectrum of the Federal Government are working cohesively and how that cooperative relationship works with the private entities and how they cultivate

these relationships to continue to ensure that America's privacy is prioritized. This is a new frontier in law enforcement, but I am inspired by the work that is already being done.

I am also looking forward to hearing what our witnesses forecast as the future threat. We all understand that at present, the eminent actor is Russia, with China also playing a role. Within the Intel and Counterterrorism Subcommittee, it is important that we anticipate the upcoming risk. The only way that we can properly equip ourselves with protection and mitigation is to understand the threat that is coming. To do that, we need to know what the cyber landscape will look like now, but also in 3 months, 6 months, and years from now.

Madam Chair, thank you again for holding this hearing. I am sincerely looking forward to hearing what the witnesses have to say and the direction that we need to go and what role we can play in Congress to support your efforts and to keep America more secure. With that, I yield back.

[The statement of Ranking Member Pfluger follows:]

STATEMENT OF RANKING MEMBER AUGUST PFLUGER

Thank you, Madams Chairwoman Slotkin and Chairwoman Clarke, for holding this important joint subcommittee hearing today, and thank you to our witnesses for joining us to discuss an issue that impacts my constituents as well as those in every other Congressional district.

The United States faces an overwhelming threat from cyber crime, especially ransomware. The attacks we have witnessed over the past year on the country's critical infrastructure put the livelihood, privacy, and way of life of everyday Americans at risk.

The criminals behind these attacks are emboldened not only by the large sums they command for their ransoms, but also by the relative anonymity they are able to maintain. Groups like Hafnium, Nobelium, and REvil launch their attacks from safe havens in Russia and China. They operate because of the blind eye and even encouragement these countries offer. I was glad to see the Department of Justice's recent indictment of two foreign nationals charged with deploying REvil ransomware to attack businesses and Government entities in the United States and I look forward to hearing about the role that DHS played in that investigation. Arrests like these should serve as a warning to every cyber criminal that the United States will bring them to justice no matter where they are located.

I, like my colleagues on this committee, am keenly interested in the preventative measures the American private and public sectors should be taking to mitigate the nefarious efforts of cyber criminals. From local school systems to pipelines supplying vital energy resources across the country, these criminals have highlighted that everyone using modern technology is at risk and we all must take measures to safeguard ourselves. However, when these measures fail, it is up to members of our law enforcement and legal communities to pursue and prosecute those responsible.

When a cyber attack occurs, every minute counts. Criminal investigators and network security experts must work hand-in-glove to understand the technologies these criminals are using, as well as the specific vulnerabilities they are exploiting.

As demonstrated by the panel before us, DHS has several components dedicated to combatting cyber crime. I am looking forward to hearing about the many ways that these components and offices work within the department, as well as with other agencies, to combat this threat. DHS is doing an incredible job and I commend them for their continued efforts. However, cyber criminals continue growing and evolving, and we must do the same to fully protect our cyber networks. It is important for us to understand how law enforcement entities within DHS and across the Federal Government are working cohesively, how the cooperative relationship between the Government and private entities is being cultivated, and how American's privacy is prioritized. This is a new frontier in law enforcement, but I am inspired by the work that is already being done.

I am also looking forward to hearing what our witnesses forecast as the future threat. We all understand that at present the imminent actor is Russia, with China also playing a role. Within the Intel and Counterterrorism subcommittee it is important that we also anticipate the upcoming risk. The only way we can be properly

equipped with protection and mitigation measures is if we understand the threat coming. To do that we need to know what the cyber landscape will look like in 3 months, 9 months, and even years from now.

Madam Chairwoman, thank you again for holding this hearing. I am sincerely looking forward to hearing the witnesses' testimonies today, discussing what we are doing and what can be done better, and ensuring that we have an effective, whole-of-Government plan in place to combat the threat of ransomware.

Chairwoman SLOTKIN. Thank you, Mr. Pfluger. The Chair now recognizes the Chairwoman of the Cybersecurity, Infrastructure Protection, and Innovation Subcommittee, the gentlewoman from New York, Ms. Clarke, for an opening statement.

Chairwoman CLARKE. Good morning, everyone. I want to thank Chairwoman Slotkin, Ranking Members Pfluger and Garbarino for collaborating on this important timely hearing. I would like to thank the panel of witnesses for joining us today. Earlier this year, as Chair of our first hearing of this Congress on the ransomware epidemic because I recognize what a serious challenge it poses to our National security. At that hearing, we heard from members of the Ransomware Task Force, the president of the National Association of State Chief Information Officers, and former CISA Director Chris Krebs about what actions the Federal Government must take to address this cybersecurity crisis.

Just 2 days later, Colonial Pipeline reported it was shutting down 500—excuse me—5,500 miles of pipeline as a precaution after being hit by a ransomware attack. Reports about ransomware attacks had been simmering for years, but they reached a boiling point overnight as gas shortages—excuse me.

Madam Chair, I got a little—I am having a little technical difficulties here.

Chairwoman SLOTKIN. No problem. Madam Chair, we can hear you, but would you like us to circle back with you?

Chairwoman CLARKE. That would work a bit better.

Chairwoman SLOTKIN. Of course.

Chairwoman CLARKE. I am sorry about that happening.

Chairwoman SLOTKIN. Of course, no problem. No problem. Welcome to the modern era here. The Chair now recognizes the Ranking Member on the CIPI subcommittee, Mr. Garbarino, for an opening statement.

Mr. GARBARINO. Thank you, Chairwoman Slotkin and Chairwoman Clarke for holding this important hearing, and my good friend and colleague from Texas Mr. Pfluger. I appreciate the witnesses being here today to discuss the administration's holistic efforts to combat ransomware. Over the past several years, ransomware attacks have increased at an alarming rate.

This year alone, we have witnessed the impact of devastating attacks on Colonial Pipeline, JBS Meats, and yet another school district on Long Island where I am from. Earlier this year, both the Bay Shore and Lindenhurst School Districts in my district were hit by cyber attacks. It was recently reported that Manhasset School District on Long Island also experienced an attack in September. If the past year has taught us nothing else, it is that no entity is too small or too big to experience a ransomware attack. We all must stay vigilant to protect ourselves and our country.

This summer, I was pleased to host a ransomware roundtable in my district with local schools, hospitals, small businesses, and gov-

ernment. CISA's Region 2 team explained how CISA can help mitigate these attacks. CISA's regional teams are the agency's secret weapon to fight this. CISA has the tools and capability necessary to bolster any entity's cyber defenses free of charge.

I am committed to continuing to work with the entities in New York's 2d District and across the country to improve their cybersecurity posture in the wake of increasing threats. We must ensure DHS, particularly CISA, has the resources and capabilities to help entities to do just that.

It is also vital that the Secret Service has the authorities and resources to investigate ransomware attacks and illicit financing operations. The Secret Service's National Computer Forensics Institute provides cyber crime investigative training to State and local law enforcement, prosecutors, and judges. I look forward to hearing from the Secret Service how we can continue to leverage this critical training to bolster our defenses at the State and local level.

Ransomware attacks have devastating real-world consequences for Americans. Every minute that a hospital goes down is a minute of missed critical care. This life-threatening risk poses similar concerns for almost every industry. We need to double down in ensuring State and local entities and small businesses—we need to double down in ensuring that State and local entities and small businesses 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.

I am a proud original cosponsor of the Chairwoman's State and Local Cybersecurity Improvement Act, which would establish a grant program for State and local entities to improve their cyber posture. While we know resources for our State and local governments are necessary to reduce the threat of cyber attacks, we must ensure these funds are spent responsibly and have a meaningful impact on risk reduction. CISA plays a vital role here. This important bill is a tremendous step forward in our fight, but we can't stop there. We must adopt an all-of-the-above approach to dealing with this challenge. There is no single silver bullet.

I look forward to hearing from our witnesses today about the innovative solutions Congress could consider as we work to degrade and ultimately eliminate the viability of ransomware. Last, I want to thank Brandan Wales for his leadership as acting director of CISA for nearly 8 extremely turbulent months. Mr. Wales, your work at the helm of this agency was a tremendous benefit to our Nation. Thank you. Thank you again to both Chairs for bringing this important issue to hearing today.

[The statement of Ranking Member Garbarino follows:]

STATEMENT OF RANKING MEMBER ANDREW GARBARINO

Thank you, Chairwoman Clarke, and Chairwoman Slotkin for holding this important hearing today. I appreciate our witnesses being here to discuss the Department of Homeland Security's holistic effort to combat ransomware. Over the past several years ransomware attacks have increased at an alarming rate. This year alone we have witnessed the impact of a devastating ransomware attack on Colonial Pipeline, which led to gas shortages on the East Coast, attacks on JBS Meats, and software firm Kaseya. Imagine a similar attack on a major U.S. port, airline, or shipping company as the holidays approach.

If the past year has taught us nothing else, it's that no one is too small, no one is too big, we all must play a part in protecting ourselves from these attacks. Earlier this year both the Bay Shore and Lindenhurst school districts on Long Island were hit with cyber attacks. In August, I was pleased to host a roundtable discussion in my district with local businesses, government, and CISA's Region 2 team. CISA's regional teams are the agency's secret weapon in this fight, at my roundtable the local cybersecurity advisor and regional director explained the tools and capabilities CISA can provide to entities to bolster their capabilities, free of charge. Ranking Member Katko and I have been strongly advocating that fellow Members to conduct similar roundtables and get the word out about these essential resources.

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.

We must ensure the Department of Homeland Security, particularly CISA, has the resources and capabilities to detect, prevent, and mitigate ransomware attacks. It's also vital that the Secret Service has the capabilities to investigate ransomware attacks, as well as the illicit financing operations behind them. Secret Service also runs the National Computer Forensics Institute—NCFI. Located in Hoover Alabama, the NCFI provides training to State, local law enforcement, prosecutors, and judges with cyber crime investigative methods, and tools to talk the fight to the criminals. The cybersecurity subcommittee has a long track record of supporting the NCFI, including leading the authorization in 2017. I look forward to continuing to work with my colleagues on this moving forward.

We also 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 back-ups, developing a response plan, and updating software.

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 also must ensure these funds are spent responsibly, and has a meaningful impact on risk reduction. CISA plays a vital role here. This important bill is a tremendous step forward in our fight, but we can't stop there. I am pleased that this was included in the recently-passed bipartisan infrastructure bill.

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 SLOTKIN. Thanks. I believe we all second that. Madam Chairwoman, are we ready to go? Can I yield back to you?

Chairwoman CLARKE. We are ready to go.

Chairwoman SLOTKIN. OK.

Chairwoman CLARKE. We are ready to go, Madam Chair. As I was stating, I held our first hearing of this Congress on ransomware epidemic because I recognize what a serious challenge it poses to our National security. At that hearing, we heard from members of the Ransomware Task Force, the president of the National Association of State Chief Information Officers, and former CISA Director Chris Krebs about what actions the Federal Government must take to address this cybersecurity crisis.

Just 2 days later, Colonial Pipeline reported it was shutting down 5,500 miles of pipeline as a precaution after being hit by a ransomware attack. Reports about ransomware attacks had been simmering for years but they reached a boiling point overnight as

gas shortages occurred across much of the east coast. As spring wore on, we learned about ransomware attacks against JBS Foods, Kaseya, Brenntag, and others.

Fortunately, President Biden has made combatting ransomware a top priority since taking office. At DHS, Secretary Mayorkas announced that ransomware would be the first of the Department's 60-day cybersecurity sprints. CISA has continued to lead the way in raising awareness about how to protect against ransomware, including by supporting stopransomware.gov *[https://www.cisa.gov/stopransomware],* a website with resources for businesses and individuals with steps they can take to reduce their risk. But these actions are not limited to DHS. President Biden has committed to a whole-of-Government approach that includes the Departments of State, Commerce, Justice, and Treasury and the intelligence community. The issue of ransomware has been a topic at high-level international meetings both with our allies and with our adversaries, including Russia.

I look forward to hearing from our witnesses today about how DHS is leveraging the authorities and capabilities of its components to contribute to the administration's broader ransomware efforts. I am also pleased that Congress is stepping up to provide the authorities and resources necessary to combat ransomware. In particular, the Infrastructure Investment and Jobs Act signed into law by President Biden on Monday, includes my legislation, the State and Local Cybersecurity Improvement Act, providing $1 billion in cybersecurity preparedness grants to State, local, Tribal, and territorial governments.

Additionally, the package includes $100 million for a new Cybersecurity Response and Recovery Fund that will complement cybersecurity preparedness grants by providing State and local government victims with alternatives to making ransom payments. Together these new resources will help make ransomware a higher-cost and lower-reward endeavor.

While I wish we had taken steps to enhance State and local cybersecurity earlier, I am glad that with the support of President Biden and the Senate, this year we have finally stepped up as a partner with all levels of government to secure our critical public networks. Furthermore, after many years of debate in Congress, I am confident that we will finally enact mandatory cyber incident reporting legislation as part of the National Defense Authorization Act.

As I work with my colleagues on both sides of the aisle on this committee and in the Senate to finalize an agreement, I am eager to hear our witnesses' perspectives on how greater information on cyber incidents and ransom payments would strengthen the administration's counter ransomware efforts. It is my hope that greater information sharing in support of the administration's whole-of-Government approach to combatting ransomware will help improve our viability—excuse me—visibility into the ransomware epidemic and enhance our ability to respond appropriately.

Again, I thank our witnesses for being here today. I thank my colleagues for convening this very important hearing. I look forward to your testimony here today. With that, Madam Chair, I yield back.

[The statement of Chairwoman Clarke follows:]

STATEMENT OF CHAIRWOMAN YVETTE D. CLARKE

Good morning. I want to thank Chairwoman Slotkin and Ranking Members Pfluger and Garbarino for collaborating on this important and timely hearing. And I thank the panel of witnesses for joining us today.

Earlier this year, as Chair of the Cybersecurity, Infrastructure Protection, and Innovation Subcommittee, I held our first hearing of this Congress on the ransomware epidemic because I recognize what a serious challenge it poses to our National security.

At that hearing, we heard from members of the Ransomware Task Force, the president of the National Association of State Chief Information Officers, and former CISA Director Chris Krebs about what actions the Federal Government must take to address this cybersecurity crisis.

Just 2 days later, Colonial Pipeline reported it was shutting down 5,500 miles of pipeline as a precaution after being hit by a ransomware attack.

Reports about ransomware attacks had been simmering for years, but they reached a boiling point overnight as gas shortages occurred across much of the East Coast.

As spring wore on, we learned about ransomware attacks against JBS Foods, Kaseya, Brenntag, and others.

Fortunately, President Biden has made combatting ransomware a top priority since taking office.

At DHS, Secretary Mayorkas announced that ransomware would be the first of the Department's 60-day cybersecurity sprints.

And CISA has continued to lead the way in raising awareness about how to protect against ransomware, including by supporting StopRansomware.gov, a website with resources for businesses and individuals with steps they can take to reduce their risk.

But, these actions are not limited to DHS. President Biden has committed to a whole-of-Government approach that includes the Departments of State, Commerce, Justice, and Treasury and the intelligence community, and the issue of ransomware has been a topic at high-level international meetings both with our allies and with our adversaries, including Russia.

I look forward to hearing from our witnesses today about how DHS is leveraging the authorities and capabilities of its components to contribute to the administration's broader ransomware efforts.

I am also pleased that Congress is stepping up to provide the authorities and resources necessary to combat ransomware.

In particular, the Infrastructure Investment and Jobs Act signed into law by President Biden on Monday includes my legislation, the State and Local Cybersecurity Improvement Act, providing $1 billion in cybersecurity preparedness grants to State, local, Tribal, and territorial governments.

Additionally, the package includes $100 million for a new Cybersecurity Response and Recovery Fund that will complement cybersecurity preparedness grants by providing State and local government victims with alternatives to making ransom payments.

Together, these new resources will help make ransomware a higher-cost and lower-reward endeavor.

While I wish we had taken steps to enhance State and local cybersecurity earlier, I am glad that with the support of President Biden and the Senate this year, we have finally stepped up as a partner with all levels of government to secure our critical public networks.

Furthermore, after many years of debate in Congress, I am confident that we will finally enact mandatory cyber incident reporting legislation as part of the National Defense Authorization Act.

As I work with my colleagues on both sides of the aisle on this committee and in the Senate to finalize an agreement, I am eager to hear our witnesses' perspective on how greater information on cyber incidents and ransom payments would strengthen the administration's counter-ransomware efforts.

It is my hope that greater information sharing in support of the administration's whole-of-Government approach to combatting ransomware will help improve our visibility into the ransomware epidemic and enhance our ability to respond appropriately.

Again, I thank the witnesses for being here today and look forward to their testimony.

I yield back.

Chairwoman SLOTKIN. Thank you, Chairwoman. The Chair now recognizes the Chairman of the full committee, the gentleman from Mississippi, Mr. Thompson, for an opening statement.

Chairman THOMPSON. Thank you very much, Chairwoman Slotkin and Chairwoman Clarke for convening this hearing and for your leadership on this important issue.

We are here today to discuss the Department of Homeland Security's work as part of the Biden administration's whole-of-Government approach to countering ransomware. I am particularly pleased that President Biden is harnessing capabilities across the Federal Government to prevent, respond, mitigate, and recover from ransomware attacks.

Clearly, DHS is the agency that has the capabilities and I believe they are uniquely positioned to help address the threats posed by ransomware as well as future attacks. I am pleased that you are holding this hearing today and I look forward to testimony from the witnesses between CISA, U.S. Secret Service, and other DHS partners to protect our communities and critical infrastructure from ransomware attack. I yield back.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

NOVEMBER 17, 2021

We are here today to discuss the Department of Homeland Security's work as part of the Biden administration's whole-of-Government approach to countering ransomware. Under President Trump, cybersecurity was not prioritized. Under President Trump, the position of cybersecurity coordinator was eliminated from the National Security Council even as we say ransomware emerge as homeland security threat to our Nation's critical infrastructure.

Like with so many other National challenges, we lost ground during the Trump administration with respect to preventing ransomware and our schools, cities, pipeline, water and others in critical infrastructures are paying the price. This year has already seen crippling and costly ransomware attacks that have disrupted Federal, State, and local government, our infrastructure, and more. Across the country, we have seen hospitals struggle to carry out their life-saving work when their systems were compromised. Many of the worst attacks originate from Russian soil, and cyber criminals often operate with tacit knowledge, and even approval, from Russian security services.

To his credit, President Biden is taking this threat seriously and has repeatedly and directly called on Vladimir Putin to act with respect to Russian hackers involved in ransomware attacks on U.S. interests. In October, he convened a 2-day White House counter-ransomware summit with 30 countries to put further pressure on President Putin and announced that we "look to the Russian government to address ransomware criminal activity coming from actors within Russia." I am particularly pleased that President Biden is harnessing capabilities across the Federal Government to prevent, respond, mitigate, and recover from ransomware attacks.

From what I know of the Department of Homeland Security and its capabilities, I believe that DHS is uniquely positioned to help address the threat posed by ransomware, prevent future attacks, and track down the criminals engaged in ransomware attacks. I am pleased that Chairwoman Slotkin and Chairwoman Clarke are leading on this critical issue by holding today's hearing and I look forward to the testimony from the witnesses and hearing more about collaboration between CISA, the U.S. Secret Service, and other DHS partner to protect our communities and critical infrastructure from ransomware attacks.

Chairwoman SLOTKIN. Thank you, Mr. Chairman. Members are also reminded that the subcommittee will operate according to the guidelines laid out by the Chairman and Ranking Member of the full committee in their February 3 colloquy regarding remote proce-

dures. I now welcome our panel of witnesses. We got there, guys. We got there.

Our first witness is Mr. Robert Silvers, the Under Secretary for Strategy, Policy, and Plans at the U.S. Department of Homeland Security. Mr. Silvers leads policy and implementation plans across all of DHS's missions. He previously served as DHS's assistant secretary for cyber policy and is the Department's deputy chief of staff.

Our second witness is Mr. Brandon Wales, the executive director of the Cybersecurity and Infrastructure Security Agency. Mr. Wales is CISA's senior career executive and has served in the Department of Homeland Security for over 15 years, including as was mentioned by Mr. Garbarino, the acting CISA director, for many, many months. Thank you for that service and DHS chief of staff.

Finally, we have Mr. Jeremy Sheridan, the assistant director of the Office of Investigations at the U.S. Secret Service. Mr. Sheridan has served in numerous supervisory assignments in the field, at headquarters, and in protective divisions including as the deputy assistant director of the Office of Training, deputy assistant director of the Office of Investigations, and assistant director of the Office of Intergovernmental and Legislative Affairs.

Without objection, the witnesses' full statements will be included for the record. I now ask each witness to summarize his remarks for 5 minutes, beginning with Under Secretary Silvers.

STATEMENT OF ROBERT SILVERS, UNDER SECRETARY, OFFICE OF STRATEGY, POLICY, AND PLANS, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. SILVERS. Thank you, Chairwoman Slotkin, Chairwoman Clarke, Ranking Member Garbarino, Ranking Member Pfluger, of course, Chairman Thompson, as well, as well as the other distinguished Members. Thank you for inviting me here to testify today about ransomware. Today, I will explain the all-hands approach that this administration is taking to combat ransomware and to protect the American people.

Ransomware attackers require victims to pay to regain access to critical data, to restore operations, and to prevent disclosure of sensitive information. The downstream effects can have National-level implications as we saw when this country's gasoline supply was interrupted by the attack on Colonial Pipeline. But ransomware also hits directly into communities. It victimizes schools, hospitals, local government agencies, and small- and medium-size businesses. I agree with your comments, Chairwoman Slotkin, this is an issue that impacts ordinary Americans.

As the under secretary, I am responsible for developing our Department's approach to preventing and mitigating ransomware and to disrupting its perpetrators. I do this together with my colleagues from the Cybersecurity and Infrastructure Security Agency and from the U.S. Secret Service, who I am pleased to be joined by today. I also do this together with other Federal agency partners and with the private sector. DHS is spearheading much of the administration's effort to counter ransomware. First, we are building resilience across our critical infrastructure and private-sector businesses. We are laser-focused on helping organizations to harden

their defenses. We are sharing ransomware threat information and network defense best practices.

In March, Secretary Mayorkas ordered a 60-day cyber sprint on ransomware so that we could bolster the support that we can offer to our stakeholders. We have launched stopransomware.gov, a one-stop shop to access Federal guidance on ransomware protection, detection, and response. Second, we and our partners across the administration are being aggressive in disrupting ransomware actors. We are taking the fight to them. We are seizing their cryptocurrency, indicting them, sanctioning them, sanctioning the financial platforms that they use, and taking other steps to disrupt the infrastructure that they use to commit their crimes.

The Department of the Treasury working with other agencies has levied its first-ever sanctions against virtual currency exchanges that are complicit in facilitating ransomware payments. These designations restrict the ability of ransomware actors to launder and move ransomware proceeds. The Department of Treasury has also sanctioned individuals associated with REvil, the ransomware syndicate behind the attack on JBS Foods and the IT services firm Kaseya. The Department of Justice has seized millions of dollars in cryptocurrency from the threat actors behind prominent attacks on Colonial Pipeline and Kaseya, amongst others. The Secret Service investigates ransomware attacks and interdicts ransomware payments as part of its work on the National Cyber Investigative Joint Task Force where it leads the Criminal Mission Center.

As our third line of effort, we are engaging with international partners to counter ransomware. In October, the White House hosted a counter-ransomware summit with over 30 countries. With our partners, we reinforce responsible norms of cyber activity. We call out and confront those countries that undermine them. We share information to protect our critical infrastructure through CISA's CERT-to-CERT relationships around the world. We collaborate on investigating and arresting cyber criminals wherever they operate. All of these efforts achieve results.

The battle against ransomware is on-going and we are approaching it with resolve. We are taking an all-of-the-above approach as you said, Chairman Garbarino. Building up defenses at home, linking arms with our partner countries, and finding and routing out the perpetrators, their infrastructure, their money.

I thank the subcommittees for holding a hearing on this topic today and I look forward to your questions.

[The joint prepared statement of Mr. Silvers, Mr. Wales, and Mr. Sheridan follows:]

JOINT PREPARED STATEMENT OF ROBERT SILVERS, BRANDON WALES, AND JEREMY SHERIDAN

NOVEMBER 17, 2021

Chairwoman Clarke, Chairwoman Slotkin, Ranking Member Garbarino, Ranking Member Pfluger, and distinguished Members of the Subcommittees on Cybersecurity, Infrastructure Protection, & Innovation and on Intelligence and Counterterrorism, thank you for inviting us to testify regarding the continued threat of ransomware and the constant risks it poses to the American people. Our testimony today highlights the Department of Homeland Security's (DHS) efforts to counter these risks. These efforts are made in coordination with the administration's

counter-ransomware initiatives, and our partners in Federal, State, local, Tribal, and territorial governments, the private sector, and internationally.

Our joint testimony today reinforces that we cannot approach the problem of ransomware by looking at only one aspect of the threat. We must tackle ransomware through a comprehensive strategy that includes close partnerships with the private sector and integrates the collective efforts to:

- disrupt cyber criminals;
- build resilience of entities and individuals;
- improve oversight of and, where appropriate, enforcement against virtual currency exchanges and on-line dark marketplaces that enable the ransomware threat;
- apply diplomatic pressure on countries that harbor ransomware perpetrators; and
- forge coalitions of like-minded countries to collectively counter the threat.

All of these efforts involve international cooperation to eliminate the safe havens and opportunities for ransomware actors. Please allow us to discuss some of the efforts under way at DHS, across the U.S. Government, and with our domestic and foreign partners to combat ransomware.

THE ADMINISTRATION'S APPROACH TO RANSOMWARE

Ransomware is a financially-motivated crime. Ransomware attackers extort vulnerable organizations and individuals. They obligate their victims to pay ransoms using virtual currencies in order to regain access to critical data, restore IT functions, and prevent the stolen data from being disclosed. But the cost to society is more than the ransom. We have seen too frequently the operational disruptions and downstream National impacts that can result from ransomware. We have seen hospitals, municipal governments, schools, police departments, and other essential businesses and organizations taken off-line. Earlier this year we experienced a disruption to our gasoline supply resulting from a ransomware attack against Colonial Pipeline. And we saw certain food prices rise following an attack on a major meat processor, JBS. We recognize the stakes and are all-in to address this scourge.

The administration is spearheading a whole-of-Government counter-ransomware initiative that is working with partner nations to disrupt and deter ransomware actors while simultaneously promoting resilience and cybersecurity across our critical infrastructure and private businesses. Through this initiative, we are targeting criminal actors for apprehension and prosecution. We are targeting and dismantling the infrastructure used to conduct these attacks.

We are targeting the illicit financial gains these actors seek, as well as the unlawful financial networks used to move, launder, and conceal illicit profits. We are increasing resilience in our critical infrastructure, and the private and public sectors in general, through cyber education and awareness and sharing information on tactics used by our adversaries. One example of these efforts is the U.S. Treasury Department's recent announcement of sanctions on the Russia-based SUEX cryptocurrency exchange for facilitating transactions involving illicit proceeds from at least eight ransomware variants. This was the first time such actions were taken against a cryptocurrency exchange. We will continue to do more to effectively disrupt this threat.

THE DEPARTMENT OF HOMELAND SECURITY'S SPRINT TO COMBAT RANSOMWARE

We are here today to talk about the significant efforts DHS is making to support the administration's counter-ransomware initiative. In February 2021, Secretary Mayorkas issued a call for action to tackle ransomware more effectively. In March, DHS launched a 60-day sprint to combat ransomware.[1] This was the first of 6 cyber-focused sprints and was intended to elevate existing efforts and remove roadblocks hampering progress. Through the Secretary's leadership and leveraging the unique capabilities of DHS components, we took action to increase resilience, and disrupt criminal use and development of ransomware.

During this sprint, Secretary Mayorkas and Attorney General Garland participated in the annual Five Country Ministerial, which issued a "Ministerial Statement Regarding the Threat of Ransomware."[2] Many components within DHS played an active role. The U.S. Secret Service held a virtual cyber incident response sim-

---

[1] See *Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience* (March 31, 2021), available at *https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience.*

[2] See *Five Country Ministerial Communiqué* (April 9, 2021), available at *https://www.homeaffairs.gov.au/news-media/archive/article?itemId=596.*

ulation with State and local governments focused on ransomware, and the Cybersecurity and Infrastructure Security Agency (CISA), in partnership with the U.S. Treasury Department, engaged with the cyber insurance industry on ransomware. The U.S. Coast Guard held exercises to synchronize Coast Guard and State incident response, and numerous U.S. Immigration and Customs Enforcement (ICE) symposia, panels, and discussions were held on cyber crime and ransomware.

As a natural progression of the sprint, in July DHS led, along with colleagues across the U.S. Government, the launch of "StopRansomware.gov,"[3] our official central website for resources from across the Federal Government community to tackle ransomware more effectively. The purpose of this website is to help public and private organizations defend against the rise in ransomware attacks by providing guidance on protection, detection, and response all on a single website.

The Department's sprint efforts are on-going. Through multiple DHS agencies, we continue to work with our State, local, Tribal, and territorial partners to build awareness, promote preparedness, and improve resilience. We continue to work with these same partners to build investigative capability through programs like the National Computer Forensic Institute (NCFI). We continue to promote preparedness and resilience across critical infrastructure and across the private sector.

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY EFFORTS ON RANSOMWARE

One of CISA's core functions is to foster such resilience. It played a leading role for DHS in launching "StopRansomware.gov." In January 2021, CISA launched a "Reduce the Risk of Ransomware" awareness campaign.[4] This campaign promoted resources and best practices to mitigate the risk of ransomware and focused on supporting COVID–19 response organizations and K–12 institutions. Further, CISA expanded its publicly available information to include a ransomware guide, fact sheets, tool kits, on-line training resources, and educational webinars.

CISA has also taken many proactive steps to prevent the ransomware threat. These efforts include hundreds of engagements focused on cybersecurity and combatting ransomware. CISA routinely engages with State, local, Tribal, and territorial partners, including events specifically for Governors and county leaders; and for the private sector. In addition, CISA continues to release cyber alerts containing technical details and mitigation measures. These alerts, often issued jointly with interagency partners, provide timely information about current security issues, vulnerabilities, and exploits. Several recent examples include information on BlackMatter ransomware, Conti ransomware, and on-going cyber threats to water and wastewater systems. Effective confrontation of the ransomware threat relies on visibility and awareness, and CISA provides that through email and other subscription services.

Visibility and awareness also require information sharing and collaboration. CISA launched the Joint Cyber Defense Collaborative (JCDC) to lead the development of the Nation's cyber defense plans, which outline activities to reduce the prevalence and the impact of cyber intrusions such as ransomware. JCDC promotes National resilience by coordinating actions to identify, protect against, detect, and respond to the malicious cyber activity targeting U.S. critical infrastructure or national interests. Building on the authorities included in the Fiscal Year 2021 National Defense Authorization Act, the JCDC includes the joint cyber planning office, but recognizes that that there is a full suite of capabilities necessary to truly make a difference for our Nation's cybersecurity posture. The JCDC will bring together leading technology, communications, and incident response companies, as well as all relevant Federal agencies, to unify and integrate prevention and response planning. The JCDC is uniquely the only Federal cyber entity that proactively provides visibility into the common operating picture of the threat environment through partnership with the private sector and the Federal cyber ecosystem.

THE U.S. SECRET SERVICE EFFORTS ON RANSOMWARE

For more than 150 years, the U.S. Secret Service has investigated financial crimes. Following the proceeds from ransomware attacks is no different. With the support of its partners, the Secret Service has shut down a number of illicit cryptocurrency exchangers that facilitated the laundering of criminal proceeds, in-

---

[3] See *New StopRansomware.gov Website—The U.S. Government's One-Stop Location to Stop Ransomware* (July 15, 2021), available at *https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/new-stopransomwaregov-website-us-governments-one-stop-location.*

[4] See *CISA Launches Campaign to Reduce the Risk of Ransomware* (Feb. 16, 2021), available at *https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware.*

cluding proceeds from ransomware. The Secret Service's successes include working with partners to shut down Western Express in 2013 and BTC-e in 2017,[5] both of which served as key laundering platforms for cyber criminals.

Secret Service Cyber Fraud Task Forces (CFTFs), located domestically and internationally, are at the forefront of investigating cyber-enabled financial crimes. CFTFs partner with State, local, Tribal, and territorial (SLTT) law enforcement, private and public sectors, to include financial institutions, and academia. An additional significant effort is made through the NCFI. This Federally-funded facility provides training courses to SLTT law enforcement, prosecutors, and judges at no cost to the attendees or their agencies. Attendees, who receive training on cyber response and investigation, to include ransomware, act as force multipliers for Secret Service CFTFs. Operation Zydeco in 2019[6] is one such example, where SLTT members of the Secret Service Louisiana CFTF trained by NCFI responded to a ransomware attack targeting a sheriff's office. In October 2021, NCFI hosted a virtual cyber incident response competition to test the technical skills of SLTT law enforcement as a Federal/State group responding to a ransomware incident.

Today, the U.S. Secret Service coordinates, integrates, and shares information on its ransomware cases through the National Cyber Investigative Joint Task Force (NCIJTF), where a Secret Service agent leads the Criminal Mission Center. Through the NCIJTF, the Secret Service works hand-in-hand with partners from the Departments of Justice, State, the Treasury, and other domestic and foreign partners. This collaborative approach to investigating cyber crime is essential in pooling Government resources and skill sets to best combat ransomware actors and their networks. The Secret Service also continues to reinforce its international partnerships.

Ransomware actors are geographically dispersed; disrupting them requires the cooperation of international law enforcement agencies to locate, arrest, and hold these actors accountable for criminal activity. The Secret Service fosters collaboration, developed and built upon years of cooperation, through direct partnership with foreign law enforcement agencies and international law enforcement organizations like INTERPOL and Europol. An example of this was the February agreement of a Canadian-American citizen, Ghaleb Alaumary, to plead guilty to two counts of conspiracy to commit money laundering, including laundering funds from a 2019 North Korean-perpetrated cyber-heist of a Maltese bank.[7] In September, Alaumary was sentenced to more than 11 years in Federal prison and was required to pay more than $30 million in restitution to victims.[8] This case highlights the transnational nature of criminal organizations engaged in these sorts of crimes.

Efforts by the Secret Service, ICE, and other law enforcement partners to hold criminal actors responsible are on-going, as well as efforts to strengthen law enforcement capabilities to counter the threat of ransomware.

INTERNATIONAL EFFORTS

The United States cannot combat this threat alone. We must continue to work alongside our international partners, strengthening existing relationships, and forging new ones. Together we must stand united to support the adoption of, and adhere to, international cyber norms and condemn countries who violate these norms or harbor cyber criminals, or support their criminal activities.

In late October, the United States hosted a Counter-Ransomware Initiative meeting with like-minded international partners from more than 30 countries. Delegates had an open discussion on common challenges, approaches, and opportunities to advance international cooperation to achieve shared goals. DHS, together with the Departments of Justice, State, and the Treasury, also recently participated in the initial meeting of the U.S.-E.U. Ransomware Working Group. This effort is the result of an agreement between the Secretary of Homeland Security and Commissioner

---

[5] See *Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox* (July 26, 2017), available at *www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged.*

[6] See *Louisiana Sheriff's Office Targeted in Cyberattack Attempt* (Dec. 16, 2019), available at *https://apnews.com/article/c2c78e08b8e82791ada335ce9f8dbf5f.*

[7] See *Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe* (Feb. 17, 2021), available at *https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.*

[8] See *International Money Launderer Sentenced to More Than 11 Years in Prison for Laundering Millions of Dollars in Cyber Crime Schemes* (Sept. 8, 2021), available at *https://www.justice.gov/opa/pr/international-money-launderer-sentenced-more-11-years-prison-laundering-millions-dollars.*

Johannsen of the European Commission to explore joint solutions to this global problem. The Department also participates in a ransomware working group with the Republic of Korea and through the Five Country Ministerial. These meetings and the scope of participation confirm ransomware is not just an issue for the United States.

The Department continues to work together with like-minded international partners to target, identify, and prosecute cyber criminals, disrupt their IT infrastructures, and shut down financial networks used to launder illicit proceeds. We collaborate and share active threat intelligence and cybersecurity best practices to reinforce international societal norms for responsible behavior in cyber space and call out countries who choose not to follow these norms and instead harbor criminal cyber actors or facilitate criminal behavior.

LEGISLATIVE INITIATIVES TO ASSIST ON RANSOMWARE

We commend Congress for passing the Infrastructure Investment and Jobs Act, which includes funding to increase cyber resilience for critical infrastructure that will help prevent ransomware attacks. We also acknowledge and applaud some of the on-going efforts in Congress that would significantly help in the fight against ransomware.

Cyber Incident Reporting Legislation.—Our ability as a Department to bolster resilience and investigate criminal actors depends on us learning about ransomware attacks and other malicious cyber activity. As such, we support legislation requiring the reporting of cyber incidents. This information is critical for understanding National risk and taking actions to disrupt and deter additional malicious activity. We cannot accurately address a problem if we do not understand its scale and scope. Cyber incidents are underreported. Additional legislative steps and new authorities are necessary to understanding the full scope of the ransomware problem.

Support for the Training of State, Local, Tribal and Territorial Law Enforcement.—We appreciate Congress' continued support for the cyber training of SLLT law enforcement. Centers such as the NCFI provide critical cyber investigation skills to our partners who are often the first responders to ransomware attacks and act as force multipliers.

Law Enforcement Capabilities to Counter Cyber Crime.—The U.S. Secret Service and ICE's Homeland Security Investigations have robust capabilities to investigate criminal cyber activity, including ransomware attacks. Expanding these capabilities to include investigating money laundering associated with digital assets would give the Department an additional tool to prevent cyber criminals from profiting from their illicit gains.

These legislative actions would increase our ability to address the threat posed by ransomware.

CONCLUSION

DHS is committed to countering the threat of ransomware facing our country, our citizens, and our allies around the globe. We are grateful for the continued support of Congress and to our fellow departments and agencies for their support in this effort. Together we can increase cyber resilience and disrupt and hold accountable those who perpetrate these acts. Thank you again for the opportunity to testify today and we look forward to your questions.

Chairwoman SLOTKIN. Thank you for your testimony. I now recognize the Executive Director Wales to summarize his statement for 5 minutes.

STATEMENT OF BRANDON WALES, EXECUTIVE DIRECTOR, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. WALES. Thank you. Thank you, Chairwomen Slotkin and Clarke, Ranking Members Pfluger and Garbarino, and Chairman Thompson for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency. I look forward to discussing CISA's efforts to elevate the Nation's security and resilience against ransomware attacks.

As you know, CISA is the National coordinator for critical infrastructure, security, and resilience, responsible for reducing risks to

digital and physical infrastructure that the American people rely on every hour of every day. Within the overall administration's approach to countering ransomware, we are focused on bolstering resilience. But unfortunately, strengthening resilience to withstand ransomware attacks is arguably the most difficult element of our collective efforts as it ultimately relies on changing human behavior. While certain steps such as spotting phishing attempts and implementing multi-factor authentication or patching vulnerabilities are easily implemented at the individual level, they are much more difficult to implement in community, business, or organization-wide. Building resilience requires a long-term investment in people, processes, and technology. Every organization that wants to avoid being a victim of ransomware, must invest in the practices that will keep their customers, their systems, and their data protected.

The question that we need to be asking ourselves is what we can do to have an impact now? I point to three things. First, we must give people the tools and guidance that they need to increase their resilience and security. That is why CISA is working to raise awareness and promote basic cyber hygiene across tens of thousands of businesses and Government agencies throughout the country. But CISA cannot raise our collective baseline of awareness and resilience alone. Which is why CISA partners daily with other agencies, such as the FBI and the Secret Service, to evaluate threats and vulnerabilities, develop guidance, conduct outreach, and respond to incidents.

For example, earlier this year, CISA and the Secret Service conducted a Cyber Incident Response Simulation Workshop with State and local governments focused on ransomware. As an example of a city taking full advantage of what DHS, CISA, and the Secret Service have to offer to manage ransomware risk, we have provided a sustained partnership in cybersecurity support to the city of Los Angeles and its 44 departments serving over 4 million residents in the form of cyber information sharing, threat training, assessments, and network defense services. The Los Angeles partnership is an example of what we can replicate across the Nation.

Additionally, earlier this summer, we led the interagency development and launch of stopransomware.gov, the U.S. Government's official repository for resources from across the interagency to help public and private organizations tackle ransomware more effectively. To date, stopransomware.gov has had more than 455,000 page views and our ransomware readiness assessment tool has been downloaded nearly 15,000 times. Second, because vulnerabilities are wide-spread across technology environments, it is increasingly challenging for organizations to prioritize which vulnerabilities to fix first. Last week, we released the binding operational directive, which established a dynamic CISA-managed catalog of more than 300 known exploited vulnerabilities and requires Federal agencies to remediate such vulnerabilities within specific time frames. While aimed at the Federal Government, we strongly encourage every organization to adopt this directive and prioritize mitigation of vulnerabilities listed in CISA's public catalog as we continually identify newly-exploited vulnerabilities.

Third, we must drive impact at scale if we hope to achieve the resilience we seek. Critical to that effort will be our partnerships

with key players who can help us achieve broad-based effects. We recently launched the Joint Cyber Defense Collaborative, or JCDC, a partnership between key Federal agencies and private-sector companies to see across networks and industries to help us identify emerging threats, provide actionable information, and take action at scale to reduce the risk of compromises of all types.

Finally, and perhaps most importantly, using our role to leverage expansive information-sharing authorities to ensure early warning of threats and attacks. For example, just this morning CISA, the FBI, the Australian Cybersecurity Center, and the U.K.'s National Cybersecurity Center released a joint cybersecurity advisory highlighting on-going malicious activity associated with the government of Iran. We have observed that these actors exploit Fortinet and Microsoft Exchange proxy shell vulnerabilities to gain initial access to systems to advance follow-on operations, which include the deployment of ransomware. We urge critical infrastructure organizations to apply the recommendations listed in the advisory to mitigate those vulnerabilities.

While this advisory is based on an analysis of multiple incidents that CISA and the FBI supported, unfortunately today, we receive information on only a fraction of incidents. This hampers our ability to conduct critical analysis, spot adversary campaigns, release mitigation guidance, and provide timely response, leaving critical infrastructure vulnerable. That is unacceptable. Providing incident information to CISA and our Federal partners quickly allows us to enrich it and get it out broadly and protecting future victims and raising the baseline of our Nation's cybersecurity. I urge Congress to move quickly on the urgent priority of adopting incident notification legislation.

In closing, our Nation is facing unprecedented risk from cyber attacks undertaken by nation-states and criminals. In response and with your partnership and support, CISA will continue to lead our National call to action. Thank you for the opportunity to appear today and I look forward to your questions.

Chairwoman SLOTKIN. Thank you for your testimony. I now recognize Assistant Director Sheridan to summarize his statement for 5 minutes.

STATEMENT OF JEREMY SHERIDAN, ASSISTANT DIRECTOR OF INVESTIGATIONS, U.S. SECRET SERVICE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. SHERIDAN. Good morning, Chairman Thompson, Chairwoman Clarke, Chairwoman Slotkin, Ranking Member Garbarino, and Ranking Member Pfluger, and Members of this committee. Thank you for inviting me to testify on the role of the Secret Service, the risk posed by ransomware, and our approach to countering this threat.

I lead the Secret Service's investigative teams in our 160 global offices, which are combating transnational cyber crimes like ransomware. In fiscal year 2021, these investigative teams responded to over 700 network intrusions, prevented over $2 billion in financial losses, and returned over $54 million to victims through asset forfeitures. These outcomes illustrate one aspect of the Secret Service's role in managing risk and preventing crimes

like ransomware. Since the agency's founding, our primary investigative mission is to safeguard the integrity of U.S. financial systems, while our protective mission implements measures to prevent harm to the persons, locations, and events we protect, including harm from cyber threats.

We accomplish our integrated mission by working in close partnership with all levels of Government and private organizations to effectively manage risk. For over 30 years, ransomware has been used to hold computers hostage and extort their users. Transnational cyber-criminal networks using ransomware are enriched, emboldened, and expanded. These criminal networks are persistent in growing threat which we can best counter by driving down the profitability of their criminal schemes. This requires both improving the security and resilience of internet users and pursuing those that engage in or enable cyber crimes.

Achieving this second aspect through criminal law enforcement is the specialty of the Secret Service. For 40 years, the Secret Service has investigated cyber crimes, long before they were even called cyber crimes. While technology has rapidly evolved, our investigative approach has remained consistent. We follow the money. In doing so, we develop detailed evidence on transnational cyber crime networks. By working with our partners around the globe, we use this evidence to ensure the most significant criminals are apprehended and face justice. Extraditing cyber criminals to the United States disrupts, deters, and prevents future criminal activity. It has also resulted in reforming some experienced transnational criminals into assets in the fight against cyber crime.

This is one reason why law enforcement action is an essential component to our National response to transnational cyber crime. Law enforcement investigations also provide additional benefits by developing indicators and warnings that we share with CISA and other partners to inform their actions. I see three priorities for law enforcement to aid in countering ransomware. All three of which would benefit from Congressional action.

First, reduce the profitability of ransomware campaigns by improving the ability of law enforcement to detect and interdict criminal crime proceeds. With the support of Congress, the Secret Service is making significant investments in the tools, training, and processes to empower our cyber fraud task forces to rapidly detect and seize the proceeds of cyber crime. Enacting the Anti-Money Laundering Act of 2020 was a critical component in these efforts. But further legislative action could aid in ensuring we have the authorities and capabilities to most effectively combat the money laundering activity that is fueling the growth of transnational cyber crime.

Second, law enforcement, particularly State and local law enforcement, act as first responders to ransomware. They are a part of our local communities and can respond quickest when called by those affected by ransomware. Since 2008, the Secret Service has developed the cyber investigative capabilities of our State and local partners by training and equipping them at the National Computer Forensics Institute. However, this critical program requires Congressional reauthorization prior to September 2022 to ensure that training meets the growing demand.

Third, we must dramatically intensify international law enforcement cooperation to investigate, arrest, and prosecute those engaged in transnational cyber crimes, including ransomware. The Secret Service is fortunate to have close and collaborative relationships with numerous law enforcement agencies around the world from Europol to South Africa to Australia. These partnerships allow us to pursue transnational criminals, their associates, and their assets wherever they may reside or travel to. These partnerships depend on continued Congressional support for our international operations.

In closing, I want to stress that ransomware is a threat to every community. It is being used to disrupt schools, city governments, local police departments, critical infrastructure, and other essential services both here at home and abroad. Progress is possible but requires a commitment to prioritize this issue both domestically and internationally as one of shared interest. I thank the committee for holding this important hearing and for your continued support of the U.S. Secret Service and our partners in countering cyber crime. I look forward to working closely with you and with other Members of Congress on our shared priorities and welcome your questions.

Chairwoman SLOTKIN. I thank all the witnesses for their testimony. I will remind the subcommittees that we have 5 minutes to question the panel. I will now recognize myself for questions.

So, to the panelists, you know, in June, the President laid down a very clear marker with Vladimir Putin that we will hold Russia responsible for stopping ransomware attacks coming out of its territory regardless of who is committing them against the 16 critical U.S. infrastructure sectors. The President noted that "within the next 6 months to a year, we would hope to see the impact of our engagement with Russia on cybersecurity." Given what we all just said that Americans are on the front line when it comes to ransomware attacks, can you tell us, have we seen a change in the ransomware threat coming out of Russia hitting U.S. critical infrastructure in the past 5 months? Have the attacks gone up, gone down, or stayed the same? Mr. Silvers.

Mr. SILVERS. Thank you, Madam Chairwoman. We have been clear with Russia that actions will speak louder than words. On the trends, it is difficult to assess because the vast majority of ransomware incidents are not reported to the Government. So, we are laser-focused on getting the data and we are doing that two ways. One by enhancing our information-sharing programs with the private sector so we can get more of it. The second is by working very closely with Congress on the mandatory incident reporting bill that is being worked as part of the NDAA process, which would actually be transformative in this respect in that it would get us the data we need to make these kinds of assessments that you expect to see in your oversight role.

Chairwoman SLOTKIN. OK. So, we are going to get the data and I understand we need to get more data. But based on the data you have today in your hands, right, understanding it is imperfect, it is 5 months after a Presidential summit, have you seen attacks go down, go up, or stay the same?

Mr. SILVERS. I can't make a definitive assessment at this time. As we have discussed in our conversations, Madam Chairwoman,

you are correct that different experts have spoken in different ways about what they have seen and I think for that reason, it is important we get to ground on the data.

Chairwoman SLOTKIN. OK. So, we all work in jobs where we are evaluated based on our success or failure. What are the metrics that you can tell the American public and this committee that you will be using to determine whether attacks are going up or going down? Whether Russia is taking action or not. Because it is one thing to say we are going to take action and to demonstrate strength. It is another thing to actually have the data to back it up. So, a year from now, if you get all the things you want, what are the metrics that will help you evaluate whether things are going up or going down?

Mr. SILVERS. Thank you, Madam Chairwoman. I think some of the metrics include number of ransomware strikes. We are actively looking at sources to collect that from, including reporting to the Federal Government, but also working with, for example, private cybersecurity companies, with insurance companies who have a role in the ransomware payment ecosystem, with our monitoring of dark web forums that list ransomware activity. Through all that, we are pulling together what we believe are the best available data. The incident reporting bill will be truly transformative in helping us to do that. But I think 1 year out, we clearly will be much further along.

Chairwoman SLOTKIN. OK. Well, I would expect that 1 year out from that summit, we will be back here having that conversation with metrics to basically assess what has happened in the year since. If the United States knew that actors, criminal actors were emanating from our soil and attacking another country, we would act. I don't see any evidence that Russia is actually helping us on this score.

Turning to a different subject. I was shocked last week or 2 weeks ago to have a bunch of superintendents from Michigan, K through 12 superintendents come into my office. Every single one of them had been the victim of a ransomware attack. That means they had children's personal data in their hands, these attackers, and they had to pay the attackers in order to get them back, to get the personal data back. Folks like Ken Gutman, he is a superintendent of Wild Lake Consolidated Schools in Oakland County, a part of which I represent, 13,000 students and were hit with this ransomware attack last October.

Explain to the American public how their Government helps them when that superintendent wakes up, his data has been ransomed, someone's asking for money, who does he call? What does he do? What is the first move when that superintendent's been hit?

Mr. SILVERS. Thank you, Madam Chairwoman. This is a Main Street issue. It hits communities and we have to have our services be accessible to communities so that people who are not incredibly sophisticated in these issues can be helped by them. That is why we created a one-stop website, stopransomware.gov, that State and local school districts, police departments, hospital systems, can go to. They can find prevention advice so they can get ahead of it. They can also find response advice so that if they are hit, they know who to reach out to and can avail themselves of the services

that CISA provides for response and that, for example, the Secret Service provides for investigating the crime.

Chairwoman SLOTKIN. Great. Sure, do you want to add something very, very briefly because my time has expired.

Mr. WALES. Sure, just very briefly. The most important thing that I would hope that you can convey within your districts to your constituents is time to focus on ransomware is not after you have been hit. Because after you have been hit, your options are extremely, extremely limited. There is not a lot that anyone is going to be able to do that is going to be able to fix underlying problems. Some adversary already has your data——

Chairwoman SLOTKIN. Mm-hmm.

Mr. WALES [continuing]. In that environment. That is going to be an extremely challenging situation for any organization whether it is a Government, a school district, or a business. The time to start focusing on ransomware is before. It is right now today one of the things they can do to make that eventuality less likely to happen.

Chairwoman SLOTKIN. OK. Thank you very much. I now recognize the Ranking Member, Mr. Pfluger, for questions.

Mr. PFLUGER. Thank you, Madam Chair. I appreciate the discussion that we are having here today. I want to open up a discussion on the time to focus on this issue, the time to focus on preventing it. I would like to say that I think that the most important piece of that is deterrence. We have to have the technical capability, but we also have the political will to hold those accountable. So, I want to ask each of you just to respond whether or not when you look at something that happened in the D.C. Metropolitan Police Department where they were looking to extort the department, publish sensitive information about officers, including personal information, is this an act of terror? These are tactics that are commonly used. Is this a form of terrorism? Is it a crime? Are we getting into an act of war? What is you all's—very quickly, because I want to explore this.

Mr. SILVERS. Mr. Chairman, it is most certainly a crime and a heinous crime and one that is not just an ordinary crime, but also can raise to the National security level, I believe. That is why I believe you have seen what is a National security response. I agree on the importance of deterrence. I want to make an important point, which is—and it also goes to Chairwoman Slotkin's question—we have been quite direct with the Russian Government. But we are not sitting around and waiting for the Russian Government to act. We have communicated that if they will not act against those taking this action from their territory, we will take those actions. We are doing so. Those have been announced and some have not been announced in recent months, including cryptocurrency wallet seizures, indicting people, putting them on the run. The noted cybersecurity expert, Dmitri Alperovitch, has said that one of the keys here is to making ransomware criminals feel paranoid, scared, not trusting those around them. That is what we are doing to disrupt.

Mr. PFLUGER. I think to Madam Chair's point, we need to see the metrics that tell us whether or not it is being taken seriously and having an effect. Mr. Wales, is this crime? Is it terror? Is it war? I mean, the Colonial Pipeline, had that been a kinetic weapon that

was used on the Colonial Pipeline and the effects were the exact same, that would be an act of war in this country.

Mr. WALES. You know, I think that is a little bit beyond CISA's purview. But I would certainly say that it is a National security imperative that we prevent any adversary from disrupting our critical infrastructure. That is the kind of work that we are doing every day in partnership with our colleagues here at the table and elsewhere in Government.

Mr. PFLUGER. From CISA's perspective, do you see this as crime, terror, or otherwise?

Mr. WALES. You know, I think crimes are dictated by statute and my colleagues in the law enforcement community could probably tell you better than me what, you know, what is a crime and what is not. But clearly, these are crimes. Clearly, they were designed to inflict terror on their victims because they are trying to extort money out of them. The more that they could make their victims scared about what they are going to do with their information or locking up their systems and jeopardizing their businesses or the organizations they manage, makes it more likely that a victim will pay.

I think going to your earlier point, as long as ransomware is a viable tool to raise money, as long as they continue to be paid, people will continue to flock to this. So, we may take some off the table, which we have done effectively including in the last several weeks. New people will get into this because it continues to be a lucrative way of raising money because it has become a matter of paying—over the last several years, businesses have paid it as just a cost of doing business. That has resulted in the epidemic that it is today.

Mr. PFLUGER. Mr. Sheridan.

Mr. WALES. As long as it is——

Mr. PFLUGER. I am sorry to interrupt.

Mr. WALES [continuing]. That kind of thing where we are going——

Mr. PFLUGER. We are limited on time. Mr. Sheridan, your thoughts?

Mr. SHERIDAN. Yes, I would just expand on what my colleagues have said. Sir, we are deterring criminal actors through prosecution, judicial action, and asset seizure, demonstrating that no one is beyond the reach of law. Metrics have been brought up multiple times. It is recognized we need better measurement for net assessment results. But we use some quantifiable metrics in the Secret Service. We have conducted over 937 arrests for cyber fraud activities. We prevented more than $2 billion in fraud loss. We have seized more than 3.5 million of financial accounts that have been used for illicit activities. Seized $129 million. Returned more than $55 million to victims. We do have quantifiable metrics in this space. They aren't universally applied across all law enforcement entities. But we are making impact and I think those numbers demonstrate that in partnership with CISA, the FBI, and other law enforcement members.

Mr. PFLUGER. Well, this is a—there is time—the time is now for a bold moment. I think DHS needs to take the lead on this. We need to have a discussion about what this is and how we deter. I

am very concerned about whether or not we are actually able to hold people accountable inside Russia. We want to see and hear and understand the specifics of those instances and how that effect is actually being—is making headway to prevent our businesses. I don't think it is limited to 16 categories. I think that any business, any industry, any person that is terrorized by these tactics and held hostage and then forced to make a payment to the benefit of a criminal organization, terrorist organization, or State actor, is wrong. So, we are looking for DHS to make a bold statement to make recommendations to the President and to then have that deterrent as rhetoric backed up with the technical capability to prevent this. Thank you, Madam Chair.

Chairwoman SLOTKIN. The Chair now recognizes Chairwoman Clarke for 5 minutes of questioning.

Chairwoman CLARKE. Thank you, Madam Chair. The State and Local Cybersecurity Improvement Act, which provides $1 billion in grants to State, local, Tribal, and territorial governments to enhance their cyber defenses was included recently in the recently enacted bipartisan infrastructure package. I introduced this legislation to give State and local governments the ability to defend themselves against cyber criminals who have been relentlessly attacking them.

But funding alone is not enough. CISA must assist State and local governments in using this new funding and most effectively and efficiently. Mr. Wales, can you share with us about what CISA will be doing to ensure that funding is spent in ways that effectively address State's cyber risks and that we have a coordinated approach to enhancing State and local cybersecurity Nationally?

Mr. WALES. Thank you, Chairwoman Clarke. I want to really thank you for your leadership on this. We believe that the cybersecurity grants for State and local communities is really going to be a game-changer in dramatically enhancing the security of our communities throughout the country. Even before the bill was signed by the President, we had been working with FEMA to begin to map out what the plan is to roll these grants out over the next year.

We, within CISA, are working to better identify what are the priorities that we want States and locals to focus on? What does the planning architecture need to look like for States as they develop their State's cybersecurity plan? What are the priorities as that money flows down into local communities? Making sure that we are thinking through how do we get our, CISA's, field-based personnel ready to support State and locals as they begin to think about, plan, and implement the funding that will come along with these grants. You know, I think up front——

Chairwoman CLARKE. So, Mr. Wales,——

Mr. WALES [continuing]. There is a lot of unevenness——

Chairwoman CLARKE [continuing]. Have you——

Mr. WALES [continuing]. So, it is a matter of getting everyone to a common baseline.

Chairwoman CLARKE. So, Mr. Wales, have you considered already cybersecurity improvements that you will encourage grantees to prioritize? Related to that, what to collaborations with the private sector are there any recent success stories that you can share?

Mr. WALES. Sure. So, on the first question related to the early priorities, and I think a lot of those we hit on often, which is how do you get to a baseline level of cybersecurity? So, how does a State put in place and a community put in place the right level of multi-factor authentication? How does it shrink the number of privileged accounts? How does it put in place a process to close vulnerabilities as soon as they are identified? Those type of cyber essentials will be kind-of among the first priorities that we want States to invest in and making sure that they have a work force that is capable of supporting and sustaining that effort.

When it comes to our relationship with the private sector, I would say that everyday outputs that are coming from CISA are the result of our close partnership with the private sector. Even the recent cybersecurity advisories that we have released related to ransomware variants like DarkSide, and BlackMatter, and Conti ransomware, those benefit from information that we share with the private sector. Those key companies that have broad insight into the cybersecurity ecosystem who can provide us enrichment and we can get that out to the entire country. You know, in addition, I think if you look at recent announcement from Palo Alto about the identification of critical infrastructure entities that were compromised because of vulnerabilities in ZOHO ManageEngine, that was a result of information sharing from work that was done between the Coast Guard, the FBI, and CISA, with our joint cyber defense collaborative partners. They then took that information, went and looked in their own system in Palo Alto, one of our plankholder members of the JCDC went and identified additional critical infrastructure victims and is able to remediate, now able to respond or remediate those vulnerabilities. We think that this partnership both within the Government and with the private sector is beginning to pay really tremendous dividends. It is not just partnership. This is this true operational collaboration.

Chairwoman CLARKE. Wonderful. As part of the broader cyber incident reporting legislation being considered in this year's NDAA, Congress is considering a requirement that entities report ransom payments to CISA. With an estimated 70 to 75 percent of the ransomware attacks currently unreported, this mandate would ensure the Federal Government has the information necessary to investigate ransomware cases and would allow for a better understanding of the scope and patterns of ransomware attacks across the country. Mr. Wales, how would CISA share the information gained through this mandatory reporting to enhance its own counter-ransomware efforts?

Mr. WALES. Sure. So, I think that when I think about what is in the legislation, there are two pieces of it. There is the actual cyber incident information that is going to be most useful for CISA. We will then take that information working with our Federal partners and with our critical infrastructure community to get that information out in an anonymized way to be able to spot broader campaigns and to protect future victims. The actual ransom payment information will be essential to our law enforcement community, the Secret Service, the FBI, and others who can actually take that information, investigate the criminal aspects of it, and poten-

tially seize funds, trace the money, go after the perpetrators. Jeremy, I don't know if you have got additional points?

Mr. TORRES. The Congresswoman's time has expired. Congressmember Garbarino.

Chairwoman CLARKE. I thank you, Mr. Chairman, and I yield back.

Mr. GARBARINO. Thank you very much, Mr. Chairman. Mr. Wales, at the House Oversight Hearing yesterday you participated in, there was a significant amount of discussion regarding the mandatory cyber incident reporting bill in the NDAA. During the hearing, Mr. Vorndran from the FBI said it was essential for FBI to receive full and immediate access to the cyber incidents. We understand that the FBI plays an important role in investigating cyber crime and coordinating with CISA. However, as you know, Congress established CISA as the lead Federal civilian cybersecurity agency with the authority to coordinate with the private sector. The incident reporting legislation seeks to build on CISA's role. I am eager to hear your thoughts, CISA's thoughts, on giving the FBI or Department of Justice a more central role in the incident reporting legislation being debated in Congress right now. The importance of CISA's retaining its role as the lead Federal civilian cyber agency.

Mr. WALES. I don't see, you know, any of the changes that are being discussed changing CISA's fundamental role as the lead for civilian cyber defense when it comes to responding to incidents and supporting our critical infrastructure community. We have a tremendously close relationship with the FBI and the Department of Justice. Under any variation of this legislation regardless of what is passed by Congress, we will work to ensure that FBI and our other law enforcement partners and our other Federal agencies that need to have this information whether it is Treasury or Department of Energy, they will get it as soon as possible. We will work to ensure that on our end, as soon as the information comes in, it will get to the people who need the information.

In many respects, that is enshrining what we do today. CISA has not done on-site engagement with any victim that has not been fully coordinated with the FBI ahead of time. In almost all cases, that work is being done jointly today. So, we would really see this in the future as strengthening that partnership. We will have more information for both CISA, the FBI, the Secret Service, and others when we engage with our critical infrastructure community.

Mr. GARBARINO. Mr. Silvers, do you have anything to add to that, or?

Mr. SILVERS. I agree with Executive Director Wales.

Mr. GARBARINO. I appreciate that. Mr. Silvers, on Monday the DHS finally launched the Cybersecurity Talent Management System after it was authorized by Congress 7 years ago. While I appreciate this new system has significant potential to bring in the mission-critical security experts that the Department needs, it is not a silver bullet to solving the work force challenges at DHS and CISA. I remain concerned that despite this innovative tool, the Department and CISA still have onerous and duplicative vetting, elongated hiring time lines, and a lack of robust human resources organizations. Are you confident of the roll-out of the Cybersecurity

Talent Management System will make a difference? When do you expect to see tangible results?

Mr. SILVERS. Thank you very much, Mr. Ranking Member. I am confident that the CTMS, as we are calling it, will achieve tangible results. I view the hiring challenges and the shortfall of cyber talent as a National security issue. I think the CTMS is a critical component. I am glad we rolled it out just a few days ago. It is not a silver bullet. We do need to streamline other human resources processes, security clearance processes and otherwise throughout the Department. Secretary Mayorkas has been clear on that and is pursuing that as well. But I do believe that the CTMS will start to show tangible results over a period of months.

Mr. GARBARINO. Great, and I have spoken to the director recently about this and she is also very concerned. She has some ideas of where things can move along quicker and she was excited about CTMS coming out as well. Mr. Wales, would you agree? Can you weigh in? You feel confident that, you know, and I have spoken to—I was speaking to an organization of CISOs yesterday. You know, we discussed this and the pipeline, the employee pipeline for CISA and not having the proper people there right now. Can you weigh in on how CISA is going to work with CTMS?

Mr. WALES. Sure. So, you know, I think CTMS is going to be a real and powerful tool. Already, the stats I looked at this morning, we had over 650 applicants across all grades and all specializations. CTMS have already put in applications into the new CTMS system. So, we are now working to identify which of those candidates actually passed through the assessments and which ones can match up against job vacancies we have in the organization. So, it really could be an extremely powerful tool that as Under Secretary Silvers says over the next few months we can start to see tangible results from it.

That being said, you know, we are not relying only on CTMS. We have been on full court press on hiring for the past year. Just in fiscal year 2021, we brought on more net gains in fiscal year 2021 than in the previous 2 years combined times 2. So, really aggressive in kind-of filling our billets. At the same time, going to your point, and I mentioned this yesterday, we are looking at the kind-of the full process to bring people on-board and seeing what we can do internally to streamline it and where we may need additional help from Congress. But right now, we don't think that is the case, but if and when that changes, we are happy to talk to you.

Mr. TORRES. The gentleman's——

Mr. GARBARINO. I appreciate that. I want to thank you both for being here. Mr. Sheridan, I am just going to say your team in New York has been phenomenal with constituent cases. So, keep up the good work. Thank you.

Mr. SHERIDAN. Thank you, sir.

Mr. TORRES. The gentleman's time has expired. The gentleman from Rhode Island has 5 minutes.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank our witnesses for your testimony today for the job you are doing protecting the country. If I could start with Secretary Silvers. Secretary, I think part of our strategy for defending the country against ransomware needs to be focused on improving the security

of the devices and technologies that we use. I see an opportunity for Government-funded R&D in the space through critical technology security centers. A recommendation of the Cyberspace Solarium Commission, which I served also as a commissioner. Congressman Gallagher and I actually adopted this idea into an amendment in this year's National Defense Authorization Act to create 4 such centers to evaluate and test the security of devices and technologies underpinning National critical functions.

So, Secretary Silvers, I would be curious your thoughts on the merits of Government-funded R&D to improve the security ecosystem and whether you agree with the need for initiatives like critical technology security centers.

Mr. SILVERS. Thank you very much, Representative Langevin. Thank you for your leadership in the field of cybersecurity. I strongly agree in the importance of Government-funded research and development in the field of cybersecurity, in particular, cybersecurity for critical technologies, National critical functions, and other areas where you can have National-level impact from security vulnerability. I am aware of the Solarium Commission's support for that kind of funding and I support that kind of funding as well. I know you are sponsoring legislation toward that end and I would look forward to working with you on that legislation so that we can have the kind of robust research and development funding we need, which is done in part at the Department's Science and Technology Directorate, which does an amazing job in this field.

Mr. LANGEVIN. Very good, thank you for that. Continuing with you, if I could, Secretary, you spoke in your testimony about the Joint Cyber Defense Collaborative, JCDC. Which I think is a hugely important initiative at the Department of Homeland Security. In particular, I commend Director Easterly for her vision in wanting to create this along with the rest of the team, yourself included. One of the key elements that I think should be housed within the larger JCDC superstructure is the Joint Collaborative Environment, which I worked to include in the version of the National Defense Authorization Act that has passed the House already.

The JCE would improve analysis of cyber threat indicators among public and private-sector stakeholders, and in fact having public stakeholders and private-sector entities, especially in the areas of the most critical infrastructure working side-by-side seeing common threat information and such. So, can you discuss the value of the Joint Collaborative Environment within the Joint Cyber Defense Collaborative's broader mission and the importance of ensuring participation from all relevant Government stakeholders including the intelligence community?

Mr. SILVERS. Thank you, Congressman. I do believe that if Congress mandates the creation of a Joint Collaborative Environment, that should be rolled up within the structure of the JCDC. We should be unifying efforts wherever possible. I also agree strongly that all elements of Government that have a role to play should be included within those structures so that we are not siloing our activity but instead doing all the activity in a coordinated way.

Mr. LANGEVIN. So, including the intelligence community, obviously, is part of that.

Mr. SILVERS. That is correct, including the intelligence community.

Mr. LANGEVIN. Thank you. The last question I could of you, Secretary Silvers, is, you know, in thinking about how to defend the Nation from ransomware, we really can't only be thinking only about the Colonial Pipelines of the world. Small businesses, local governments, and other community institutions also face serious threats from cyber criminals. How has DHS been approaching the problem of safeguarding these institutions against ransomware? Obviously, we have seen everything from police departments and hospitals and municipalities being affected, but if you could just take that question.

Mr. SILVERS. Thank you, Congressman. You are correct. Ransomware reaches right into our communities including organizations that may not have a lot of cybersecurity resources or expertise. It is incumbent on us to make our expertise and resources accessible to those kinds of organizations like schools and hospitals and police departments. That is why we set up a one-stop ransomware website that those kinds of organizations can visit to get full spectrum support from the prevention side, which is critical, because you prevent it from ever happening if you can engage the right kinds of best practices, all the way through to response and the support we can provide through law enforcement and through CISA in the event they are targeted.

Mr. LANGEVIN. Very good, thank you. I know my time has expired. I appreciate the work that you and the team at DHS are doing to get CISA. Sorry, I didn't get to the other witnesses' also valuable testimony you provided. Thank you, Mr. Chairman. I yield back.

Mr. TORRES. The gentleman's time has expired. The gentleman from Kansas is recognized for 5 minutes.

Mr. LATURNER. Thank you, Mr. Chairman. Good morning. Thank you for being here. Mr. Sheridan, I would like to start with you. Our law enforcement performs an essential role in bolstering American cybersecurity by investigating a wide range of cyber crimes and apprehending and prosecuting those responsible. When it comes to fighting cyber crime, can you define the different roles between the Secret Service, the FBI, and HSI? How do you all work together collectively and define the different roles for me.

Mr. SHERIDAN. Certainly. The Secret Service focus by statute is to protect the Nation's financial infrastructure and financial payment systems. In our position, we utilize those statutes to, through our cyber fraud task forces located throughout the globe in order to focus primarily on payment systems, what affects the American public and the financial industry. For HSI, the focus is more on intellectual property, ecommerce, and counterfeit goods. The FBI has a broader spectrum in terms of statutory authority that touches elements across the law enforcement community.

I do think it is important that there is that overlap because cyber criminals do not specialize in one type of criminal activity that assigns itself to one statute in a very clear way. There must be overlap because ancillary crimes associated with cyber crimes that are used to facilitate the precipitating crimes, such as money laundering, human trafficking, and a full spectrum of other crimes, are

required to employ other law enforcement entities in order to partner in that overall investigation.

Mr. LATURNER. I understand the different roles, but what I am driving at here and this issue we see it come up time and time and time again, are having clear defined roles for all the entities that deal with this issue and, obviously, it is a complicated problem. We have to have different entities address it. But how those entities work together collectively and how the process is streamlined because for us, I talked about this a couple weeks ago. I have a business in my district that was held for ransom, had their data held with a ransomware attack for $900,000. They called their insurers and their lawyers and the technical experts and they tell them to pay. They get it down to $600,000. They said I think we can get it down further. He said, for heavens' sakes, we are losing a lot of money every day, a much bigger number than $600,000. So, they pay it. I said, at any point did they ask you to reach out to anyone at the Federal level? They said, no. I think that is a big problem. So, I am going to continue to talk about this because they said no because they didn't think that the Federal Government could help them in any way. They didn't think it was worth their time. So, how can those different roles as defined as they are, how can you work together better?

Mr. SHERIDAN. I agree with you that it is a big problem, sir. I will answer that question in a couple different ways. First and foremost, we have formalized structures in place for information sharing through our cyber fraud task forces, through our role and presence in the National Cyber Investigative Joint Task Force, through our role in the Joint Cyber Collaborative with CISA. Those are specifically designed to share information related to on-going investigations.

Second, in regards to the assessment that law enforcement can't help or the Federal Government can't help, I would challenge that conclusion. For us, investigation is prevention. By being brought in early in the investigative process as was referenced earlier, there is an ability for us to identify the vulnerabilities that caused the intrusion or the unauthorized access. There is the ability to identify whether the adversary is still present in the network. Our role is to assist the organization to become whole again to resume business operations. Of course, to be able to enact justice against those perpetrating the crime.

Not only that, but we have mechanisms in place through financial institutions and partnerships in order to obtain illicit funds that are in transit or going to criminal accounts, criminal wallets, criminal——

Mr. LATURNER. I want to get to one more question for the others. I would disagree with it too. But I think you would agree with the point that we have a lot of work to do.

Mr. SHERIDAN. Yes, sir.

Mr. LATURNER. To be better and to change the perception. Mr. Silvers and Mr. Wales, if you would quickly comment. This committee has been very focused on the various roles and responsibilities in the Federal Government cyber mission, particularly among the roles of the DHS Secretary, director of CISA, and the National cyber director. From your perspective, and DHS policy, what addi-

tional work needs to be done to ensure we have clear lines of roles and responsibilities that we can avoid missteps like we saw in the Federal Government's response to the attacks on Colonial Pipeline? You will have to be really quick.

Mr. SILVERS. Thank you very much, Congressman. I think actually we are working quite well together, especially since the creation, the recent creation of the National Cyber Director Office. I think what it is about is teamwork. We bring different authorities to bear, but it is about being on the same page working together and with arms linked. I think we are doing that.

Mr. LATURNER. Thank you. Thank you, Mr. Chairman. I yield back.

Mr. TORRES. The gentleman's time has expired. The gentleman from New Jersey is recognized for 5 minutes.

Mr. MALINOWSKI. Thank you, Mr. Chairman. I assume you mean this gentleman from New Jersey.

Mr. TORRES. Exactly right, Congress Member Malinowski.

Mr. MALINOWSKI. Thank you. Well, thanks to the witnesses. I know we are talking about defense of the homeland here, but I do want to turn our attention to the obvious fact that the ransomware gangs that have been wreaking this havoc are not based in Chicago or LA or New York or in England or in France. They are based in safe havens in countries where governments are either unable or, I think more likely, unwilling to confront them. I wanted to ask our witnesses a couple of questions about that.

First of all, of course, we know that a number of these operators have been working out of Russia and countries that are under the influence of the Russian government and I wanted to ask any of the witnesses whether you have seen any changes in the operations of these groups or the efforts of governments in Russia and in that neighborhood to crack down on them since President Biden issued some fairly direct warnings to President Putin at their summit in the early summer?

Mr. SILVERS. Thank you, Congressman Malinowski, for the question. We have been clear with Russia that actions are going to speak louder than words. With respect to your question about the trends, it is quite difficult to assess after a period of just a few months because the vast majority of ransomware incidents are not reported to the Federal Government. So, our focus is on accelerating our ability to collect and get at that kind of data so we can deliver those kinds of assessments to you. We are doing that two ways. One, through enhanced information-sharing programs with the private sector. We are doing that with private cybersecurity companies, the insurance industry, and others that have a role in the ransomware ecosystem. We are also doing that by working with Congress on the mandatory incident reporting legislation that is currently being part of the NDAA process. Which would candidly be transformative and ground-breaking in terms of our ability to get that kind of data as to incidents, as to ransomware payments that are made, so that we can provide better clarity on the trendlines.

Mr. MALINOWSKI. That makes sense and I strongly support that provision. But just to be clear, are you saying that absent mandatory reporting, we really have no way of knowing whether the

warnings that we have issued, the efforts, public and private that have been made to persuade those governments to crack down are working? I mean, surely, we must have some visibility into that.

Mr. SILVERS. It is incomplete, but we do have some data and it is more anecdotal. We work with what we have. I want to be clear, Representative Malinowski, that we are not sitting and waiting for Russia to act. We have communicated that we expect them to act. But if they will not, we will take action against those perpetrating ransomware from their territory. I think that is exactly what we have seen in recent months as we have announced as an administration recent ground-breaking and innovative enforcement actions to seize cryptocurrency proceeds, seize cryptocurrency wallets, sanction cryptocurrency exchanges used by ransomware actors for the first time, and indict, as such, individuals.

Mr. MALINOWSKI. No, and I applaud that and it is fantastic work you are doing. But, obviously, you know, Putin could shut these operations down in a day if he wanted to. So, this is why I focus on that. Frankly, although we don't talk about this as much publicly, I do believe that there is an offensive, not just defensive, capability that we need to be employing here.

Then, finally, you know, I have asked these questions about Russia and the former Soviet countries, but isn't it also the case that we are seeing an emergence of ransomware groups in other parts of the world like Southeast Asia, Sub-Saharan Africa, for example? If so, what are we doing working with allies in those regions to share best practices and strengthen enforcement?

Mr. SILVERS. That is very much correct, Congressman. We do see ransomware emanating from a variety of different countries. That is why one of the most important pillars of this administration's ransomware strategy has been a diplomatic effort to link arms. Recently, the White House convened over 30 participating like-minded countries to rally support for the battle against ransomware. That includes law enforcement investigation cooperation. It means reaching the arm of the law to those places. Building capacity for countries that might not have the capacity or the awareness so that we can bring more of these people to justice. That is exactly what we are doing with the Secret Service and other partners.

Mr. TORRES. The gentleman's time has expired. The gentleman from——

Mr. MALINOWSKI. Thank you.

Mr. TORRES. The gentleman from Mississippi is recognized for 5 minutes.

Mr. GUEST. Thank you, Mr. Chairman. Gentlemen, in your joint written testimony on page 1, you list out various organizations that have been impacted by ransomware. The list contains hospitals, municipal governments, schools, police departments, other essential businesses. Then you go further and you talk about some of the impacts that we have seen just within the last year of ransomware. You talk about Colonial Pipeline and the impact that it had on gas supplies and, therefore, gas prices. We talk about JBS and the impact that that had on food prices. We know that ransomware attacks and cyber attacks in general are becoming more wide-spread, more prevalent in today's society. Then today, we are talking about

a whole-of-Government approach. What we can do all levels of government, State, local, Federal, working together.

In my home State of Mississippi, we established a cyber working group. Within that cyber working group, you have not only State, Federal, and local law enforcement. It encompasses the private sector. It includes our academic universities. Also, includes the Department of Defense and our Mississippi National Guard. So, my question to any of you or to the panel as a whole, is can you talk a little bit and speak of the importance of these types of partnerships that we are seeking to put together in States across the union and the impact that they will have on combatting cyber threats?

Mr. WALES. I think that those kind of working groups are essential and actually they are going to be key part of the implementation of the cybersecurity grant program that was recently approved as part of the infrastructure bill. Each State is going to have to create or take an existing working group like Mississippi may already have used the one they have already created, make sure that there is adequate representation of the right organizations, of the right people at both the State and the local level that are going to help shape the implementation of those grants and help to focus where those go. They are going to approve the plans that are required for each State that need to be developed before the grants will be allocated.

So, and we are actively involved in a number of those cyber working groups across this country using the field-based CISA personnel, the cybersecurity advisors, and the State cybersecurity coordinators that we have out there that are designed to be that linkage between the State and local community and the broader CISA services that we offer from headquarters.

Mr. GUEST. So, let me touch on something that you brought up just a minute ago in one of your answers to Representative Malinowski's question. You talked about it and it is also contained in the written testimony about the Department of Treasury's recent announcement of sanctions on a Russian-based cryptocurrency exchange that was involved in transaction involving illegal proceeds from various ransomware attacks. I actually pulled the press release that the Treasury Department issued and it said that this particular exchange that the transactions showed that up to 40 percent of the known transactions were associated with illicit actors. Can you speak a little bit about those sanctions that were imposed and the role that not just this particular currency exchange, but some other currency exchanges are playing and what we are seeing as the ransomware attacks that are happening across the country?

Mr. SILVERS. Thank you, Congressman. It is a really important question. There is just no question that the rise of ransomware has been fueled by the availability of cryptocurrencies that allow for anonymized payments. That presents enormous challenges for law enforcement, for example. But what we have determined is that there are certain exchanges that are really being used by these threat actors because they are not governed and they don't have the kinds of financial regulatory controls that we expect to see in our financial system. So, we have not hesitated as an administra-

tion to take action against those kinds of exchanges. In fact, Treasury has sanctioned two cryptocurrency platforms in recent months. That is the first time that cryptocurrency exchanges have been subject to sanctions. I expect to see a lot more activity. A lot more aggressive disruptive action. For example, we have recently as an administration, also seized cryptocurrency wallets. Actually, seized the bitcoin or other digital tokens that are used as ransomware proceeds. So, we are taking the fight and going after these people's money.

Mr. GUEST. Just one last follow-up. My time is almost up. I know that the first cryptocurrency exchange that was sanctioned was in Russia. Where was the second one located, if you know?

Mr. WALES. It was also Russia.

Mr. SILVERS. Both Russia.

Mr. GUEST. Thank you. Thank you, Mr. Chairman. I yield back.

Mr. TORRES. The gentleman's time has expired. I will recognize myself for 5 minutes.

Mr. Silvers, I want to follow up on the questions that were asked regarding Russia from Congress Member Slotkin and Malinowski. The United States has said that it will no longer tolerate Russia's safe harbor for ransomware attacks on the 16 areas of critical infrastructure. Is that correct? Yes or no?

Mr. SILVERS. Yes, sir.

Mr. TORRES. The implication is that we will tolerate Russia's safe harbor for ransomware attacks on individuals and institutions that fall outside the 16 areas of critical infrastructure. You know, we would never make that distinction in the physical realm, why should we make that distinction in the digital realm? Like is that the policy of the United States?

Mr. SILVERS. Thank you very much, Mr. Chairman. I think the policy of the United States is that any act of ransomware is a crime and will be investigated and prosecuted. The direct——

Mr. TORRES. I am referring to Russia, not to the particular criminal actors. Are there consequences to Russia for a Russian safe harbor for ransomware attacks on non-critical infrastructure? Yes or no?

Mr. SILVERS. Mr. Chairman, the direct discussions and there have been some very direct discussions, are being led by the National Security Council directly with the Russians. I would defer to them on the content of those discussions.

Mr. TORRES. I want to go back to I understand that there is a lack of data, but there has been a lack of reporting for years. But we have enough knowledge to know that ransomware has been growing exponentially over the course of several years. Have you seen among reported incidents have you seen an increase in activity?

Mr. SILVERS. At this point, I can't give a confident assessment in the short period of time since then.

Mr. TORRES. Even among the incidents that have been reported to you?

Mr. SILVERS. So, Congressman Torres, we have seen experts who have spoken about it both ways.

Mr. TORRES. I am referring to you. You have received reports about ransomware. Have you seen an increase or a decrease? It is a straightforward question.

Mr. SILVERS. I would defer to colleagues from CISA and the Secret Service as to the types of reports they have gotten and whether there is a trend in the data that they can see.

Mr. WALES. What I would say is, and the assistant director for the FBI made this clear yesterday, based upon the reporting that is made to the Federal Government, at this time we have not seen a change in the amount of ransomware being targeted against——

Mr. TORRES. So, it remains the same.

Mr. WALES. Yes.

Mr. TORRES. So, there is no evidence that Russia is keeping its promise.

Mr. WALES. That is a broad answer in terms of all ransomware.

Mr. TORRES. OK. Well, if nothing has changed, I would treat it—I would ask this, do cyber-criminal organizations continue to operate disproportionately in Russia based on the intelligence that you have? Are those organizations—do those organizations continue to be active?

Mr. SHERIDAN. Congressman, we have a list of countries that have a more tolerant or offer safe harbor and in some cases offer outright support to cybercriminals. Russia is one of those countries. So, if your question is does Russia tolerate this? As a general answer, the answer is yes.

Mr. TORRES. Those organizations, to your knowledge, remain active.

Mr. SHERIDAN. Yes, sir.

Mr. TORRES. We have seen no, based on reported incidents, we have seen no decrease. It seems to me that Russia has broken its promise to the United States. But I am going to move on.

You know, we have known for a long time that cyber criminals can exploit the anonymous or pseudonymous nature of crypto for ransom payments, but we know from the experience of Colonial Pipeline that law enforcement, particularly the FBI, can exploit the transparency of blockchain for ransom recovery. The FBI, it has been reported, recovered most of the $4.4 million ransom that Colonial Pipeline paid. Does the Secret Service and HSI, does the Secret Service have the same technical capacity to exploit the transparency of blockchain for ransom recovery?

Mr. SHERIDAN. Yes, sir. I would say that blockchain by its very nature is transparent. The reason—I can't comment on the actual investigative techniques used for that seizure, but that reason for that seizure was not solely technical in nature. There was intelligence components involved.

Mr. TORRES. Do you think with enough technical expertise and enough public investment we could make ransom recovery the rule rather than the exception? Or is it prohibitively intensive and expensive?

Mr. SHERIDAN. That is a great question. I think we could certainly be more proficient in it. The Secret Service is, you know, employs a host of computer scientists, blockchain analysts, crypto tracers who are very adept at that exact activity. But we need to get better. We need to expand our staffing. We need to increase our

foreign presence. We need to have greater technical capability in this arena. We can certainly seize more of it. If it becomes the rule, that is really hard to assess, sir.

Mr. TORRES. I will ask one question. You know, ransomware, the rise of ransomware has multiple causes. There is ransomware as a service. Russia and Eastern Europe as a safe harbor. The anonymous and pseudonymous nature of crypto. The lack of cyber hygiene. Suppose each of you had a magic wand, which of these causes would you make disappear in order to dramatically reduce ransomware in the United States? I will start with Mr. Silvers, and that will be my final question.

Mr. SILVERS. That is a great question, Congressman. I think the rise of affiliate networks, the ransomware as a service where unrelated hackers can come together with a ransomware developer to execute a strike has really sharply escalated the volume that is hitting at us. So, I think disrupting that network it would be critical and maybe I would choose that one. I think that is what we are doing as an administration by making ransomware actors feel like they cannot trust their partners would be the test.

Mr. TORRES. I just want a quick—Mr. Wales and Mr. Sheridan, quickly, and then I have to move on to the next questioner.

Mr. WALES. Well, I will stay on-brand for CISA. You know, if we—everyone adopted basic cyber hygiene, implement the multifactor authentication, you would dramatically shrink the universe of——

Mr. TORRES. So, ransomware service, cyber hygiene, what is—what is the cause you would make magically disappear?

Mr. SHERIDAN. Partnerships with law enforcement. We need better information, better intelligence, and better communication in order to respond to these incidents.

Mr. TORRES. I appreciate the answers. My time has expired. The gentleman from Michigan is recognized for 5 minutes.

Mr. MEIJER. Thank you, Mr. Chairman, and to our distinguished witnesses for your testimony and answering our questions here today. Obviously, this is a critical subject that we have prior hearings on and I think I had the opportunity, Mr. Sheridan, to speak last time on the very same subject that Mr. Torres was asking about the ransomware utilization of cryptocurrency and in specific, my continuing concern around the use of altcoins as a way pumping and dumping to transfer revenue.

But I wanted to ask a bit more specifically—and I believe we may have another Member not on mute. Just, if that Member could mute. But, you know, we have seen foreign adversaries and bad actors exploiting U.S.-based platforms in order to conduct these cyber attacks to circumvent U.S. intelligence community restrictions, you know, individual components that may have restrictions based on domestic-based platforms relative to international that U.S. persons carve out. What more can the Federal Government do to prevent foreign entities, you know, whether it is a state actor or a nonstate actor, from doing an end-run around some of these protections that we have so that our intelligence community is not domestic-focused? What can we do to make sure that that is not being exploited for the purposes of cyber crime and specifically, ransomware?

Mr. WALES. I will start and there may be additional answers here. I think the U.S. Government is coming at this primarily from two angles. One is there was an Executive Order signed by President Trump in the waning days of the administration that was focused on improving the work with there was infrastructure, those service providers, those virtual private networks, and other cloud providers requiring them to do more kind-of let's just shorthand it with kind-of know your customer. So, improved due diligence when they are leasing their infrastructure to particularly foreign accounts. Having more due diligence on that. There was some work with the Federal Government there.

Then, second, the work that we are doing with the Joint Cyber Defense Collaborative bringing together those companies that operate this kind of global cloud infrastructure and who have broad visibility, making sure that we have got a good partnership between the Federal Government and what we know from the intelligence community, what we know from law enforcement, what we know from our network defense work. What they can see inside of their networks. The more that we can arm them the more work that they can do inside of their networks to protect their customers or their—or prevent their network from being used to being weaponized against other potential victims. So, that is part of the answer. Obviously, there is no perfect solution. This is going to require more thought and more engagement.

Mr. SHERIDAN. I would say from a law enforcement perspective increasing staffing and infrastructure in foreign locations. Also, compelling foreign exchangers and service providers to respond and provide information when we have evidence of crimes being committed. Increase accountability for ISPs hosting malicious infrastructure or other elements of criminal activity. Allowing legal process for suspects identified in non-extraditable or non-friendly countries that are willing to cooperate with U.S. law enforcement. There are still obstacles for us to do so.

Mr. MEIJER. Thank you, Mr. Sheridan. That actually feeds very well into my next question, which was to Mr. Silvers. You know, can you speak a little bit more how DHS may be utilizing deterrence on the ransomware side. Obviously, on CISA there is a strong emphasis on building up resilience on some of that basic cyber hygiene on tracking the flows afterwards in conjunction with the FBI or Secret Service. But can you speak to what initiatives or efforts DHS is trying to engage on the deterrence side to try to prevent particularly non-state actors as well from engaging in ransomware?

Mr. SILVERS. Thank you very much, Congressman, Meijer. Absolutely a critical component of this is defense. But also going on offense and really disrupting and candidly scaring the ransomware actors who are doing this so that they take their business elsewhere. I think a key component of that is law enforcement investigation, of course. We, as an administration, are also pursuing some very novel actions in terms of cryptocurrency seizures, sanctioning of cryptocurrency exchanges that are being used by these actors. As well as other activities that we wouldn't discuss in a open session like this. So, we agree and we are being aggressive.

Mr. MEIJER. I appreciate that. Thank you for that, Mr. Silvers. I think you will find full support on having a panoply of options here from the offensive to the defensive to the preventative. With that, Mr. Chairman, my time has expired and I yield back.

Mr. TORRES. The gentleman's time has expired. The gentlewoman from Texas is recognized for 5 minutes.

Ms. JACKSON LEE. Thank you so very much, Mr. Chairman. Thank you for holding this hearing. I believe I am almost in a ransomware experience now in the House of Representatives in the Rayburn Building. Forgive me for the coloration of where I am. I am almost in complete darkness, which makes this meeting and hearing more potent than I might have imagined. Let me pose a question that I hope that the Members will delve into extensively. I will say that I am an author of the original zero-day legislation that has been modified to our current set of circumstances. But I do believe that this hearing speaks to that potential of dealing with the whole-of-Government approach combatting ransomware. In the United Kingdom, there is a report that 60 percent of organizations have been hit by ransomware-as-a-service attacks in the past 18 months. Ransomware-as-a-service attacks are where one group builds a malicious code and sells it to another group to use in the virtual breaking and entering of vulnerable enterprise organization. Just a regular successful business. This may be an attempt for groups to create more activity to make it more difficult to find the more malicious and dangerous ransomware attackers.

Gentlemen, if you would answer, is the United States doing enough to collaborate with other governments to track and disrupt this sort of increasing business source of ransomware attack tools out on the marketplace? Are we seeing attacks of this nature in the United States? Is this something that is attractive and that can become very alarming? If each of you would answer starting with Mr. Silvers and then Mr. Wales and Mr. Sheridan. Thank you all very much for giving me the opportunity in the midst of darkness to ask these questions. Thank you.

Mr. SILVERS. Well, thank you, Congresswoman. I appreciate the question and to your point about the importance of international collaboration in combatting ransomware, we could not agree more strongly. That is why we have really formed a coalition of the willing of like-minded countries. We assembled over 30 of them at the White House very recently on a joint global initiative of responsible countries to combat this. That is going to take the form of joint cyber crime investigations. Sharing of cyber threat intelligence across borders. Joint actions to disrupt these criminals wherever they may operate. We couldn't agree more on the importance of the diplomatic component of this and we are on it.

Ms. JACKSON LEE. Thank you. Mr. Wales, you want to speak to the idea of ransom as we go tighten our efforts? Thank you.

Mr. WALES. No, and I think your point is right. The rise of ransomware as a service is one of the—and this goes to Congressman Torres' point earlier—it is one of the factors that has driven the acceleration of ransomware attacks because it has lowered the barrier to entry. I do not need to be as sophisticated a cyber actor if I can just rent someone else's service and use that to launch at-

tacks. I don't need to have the depth of technical knowledge and expertise in order to utilize ransomware-as-a-service platforms.

So, it has featured prominently in a number of the more significant attacks on the homeland that we have seen over the past year are driven by these what are called affiliates that utilize ransomware-as-a-service variance. I think it is because of that it had helped to sharpen the strategy we have to really go after from a law enforcement perspective working with our international partners the central hub, so the people who actually are ones who are designing the ransomware-as-a-service platforms because disrupting them could have a more pervasive effect on the ransomware ecosystem.

Ms. JACKSON LEE. Thank you. Next witness, please.

Mr. SHERIDAN. Yes, ma'am. Just to conclude. You know, we have 19 foreign offices located around the globe. We partner with Interpol, Europol, European Cybercrime Center, and other international law enforcement partners to combat this threat. As stated by my colleagues, this is a transnational organized problem that is being committed by really a small cadre who are operating, organizing, and supporting the most significant cases that we are seeing.

The ransomware actors that are the affiliates that Mr. Wales referenced are really the street-level thugs, to use a interpersonal crime metaphor. What we are trying to target are the Steve Jobs or the Bill Gates of these organizations. Our biggest challenges are the organized networks that have extensive leadership, levels of trust, and very complicated organizational structures. We target, investigate, extradite, and prosecute the top-tier criminals in those organizations. We target the networks, not just the individuals or the variants that allow financially-motivated cyber criminals to operate with impunity.

Ms. JACKSON LEE. Thank you very much. Thank you, Mr. Chairman, and I look forward to a legislative response to some of the concerns that have been raised by my question and some of the answers that have been given. Thank you so very much. I yield back.

Mr. TORRES. The gentlewoman's time has expired. I want to enter into the record testimony from Security Score Card, entitled, "Using Machine Learning to Assess Ransomware Risk."

[The information follows:]

SECURITY SCORECARD—USING MACHINE LEARNING TO ASSESS RANSOMWARE RISK

NOVEMBER 2021

Tishun Peng, PhD, Senior Data Scientist; Idin Karuei, PhD, Senior Staff Data Scientist; Bob Sohval, PhD, VP Data Science; Department of Data Science, SecurityScorecard

Ransomware is a rapidly growing global cybersecurity threat, with more than 4,000 ransomware attacks daily according to the FBI. Average ransomware payments increased by 82 percent, reaching a record high of $570,000 in the first half of 2021 compared to 2020. Additional costs associated with business interruption and recovery can more than double the total cost incurred by the targeted business.

In a previous study, SecurityScorecard identified several cybersecurity issue types that are statistically more prevalent among ransomware victims compared to other organizations. Subsequently, we developed a sophisticated machine learning model that estimates the relative likelihood of a company falling victim to ransomware attack, based on non-intrusive observations of its cybersecurity posture. The predicted

likelihood could be used to warn at-risk organizations and to assist insurance carriers offering cyber-insurance policies.

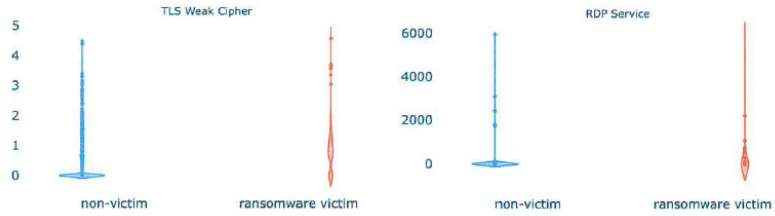
DATA AND FEATURES

Building a machine learning model to classify at-risk organizations requires labeled training data with known status (i.e. ransomware victim or non-victim).

SecurityScorecard's Threat Intelligence team continuously collects ransomware victim data by crawling the dark web, where ransomware perpetrators publish the names of victimized organizations that did not pay the ransom. The ransomware data used to train the model consisted of 963 non-paying ransomware victims covering a time period from September 2018 to August 2021. Non-victim training data were randomly selected from the more than 10,000,000 organizations monitored on the SecurityScorecard platform and matched over the same time period.

SecurityScorecard continuously collects the findings for 76 active issue types to evaluate an organization's overall cybersecurity hygiene. For each issue type, we extracted 8 informative features, including mean/max findings, mean/max findings normalized by digital footprint size, mean/max issue prevalence among comparable organizations, and the occurrences of non-zero finding and prevalence over a 3-month period leading up to the individual ransomware events. Additionally, digital footprint and employee count are also included as organization-level features.

When developing a machine learning classifier to distinguish between two classes (ransomware victim and non-victim), it is important to include features which have different distributions for the two classes. The greater the difference between the two distributions for a given feature, the more it will contribute to the final model's ability to correctly distinguish between the two classes.



The comparative distributions for two sample features are shown in the plots above. While there is overlap between the distributions for the ransomware and non-ransomware cohorts in both cases, TLS weak cipher (use of a weak cryptographic cipher) exhibits better separation than Exposed RDP Service (remote desktop protocol service exposed to the internet), which is regarded as one of the exposed services that ransomware attackers often exploit.

Machine learning algorithms find correlations between features and class labels (i.e. ransomware victim and non-victim), and build an ensemble of "weak learners" into a robust classifier.

This is a statistical process and it should be noted that "correlation does not imply causation."

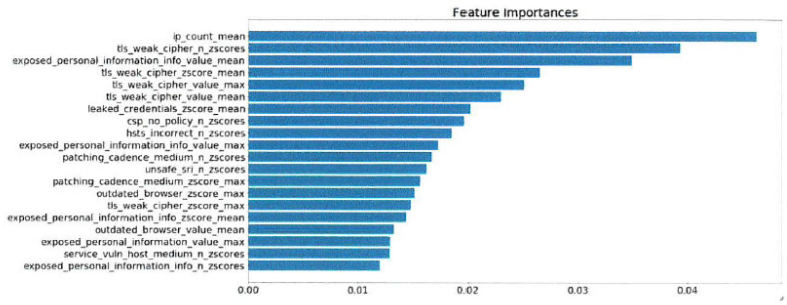
RESULTS AND DISCUSSION

Numerous machine learning models were evaluated and the random forest classification model was selected to build the classifier. The objective is to correctly identify as many ransomware victims as possible (true positive rate), while simultaneously correctly identifying as many non-victims as possible (true negative rate). The following table shows the final performance achieved and measured using 10-fold cross validation.

Metric	Mean	95% CI
True Positive Rate	80%	72% - 86%
True Negative Rate	87%	83% - 91%

The table above illustrates that the classification model correctly identified 80 percent of ransomware victims while also correctly identifying 87 percent of the non-victims. The 95 percent confidence intervals on these values are also presented.

The chart below shows a list of features ranked by their importances to classify the ransomware and non-victim cohorts. Among them, digital footprint, exposed personal information, tls weak cipher, csp no plicy, unsafe sri are ranked among the most important features. It is worth noting that they are also listed as the most prevalent issues among the ransomware victims according to the blogpost and paper published by SecurityScorecard.



CONCLUSION

SecurityScorecard has developed a machine learning model to measure the susceptibility of an organization to becoming victim of a ransomware attack. The model was trained using labeled data harvested from the dark web and SecurityScorecard's historical cybersecurity data. The model achieves a True Positive Rate of 80 percent and a True Negative Rate of 87 percent. This perfomance can assist organizations in managing the risk of ransomware attack and also help insurance carriers monitoring cyber-insurance portfolio risk.

Mr. TORRES. With that, I thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittees may have additional questions for the witnesses and we ask that you respond expeditiously in writing to those questions.

The Chair reminds Members that the subcommittees' record will remain open for 10 business days. Without objection, the subcommittees stand adjourned.

[Whereupon, at 11:38 p.m., the subcommittees were adjourned.]

○