COMBATING RANSOMWARE: FROM OUR SMALL TOWNS IN MICHIGAN TO DC

FIELD HEARING

BEFORE THE

SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

JUNE 28, 2022

Serial No. 117–64

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

48–963 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
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
MAYRA FLORES, Texas

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

CONTENTS

COMBATING RANSOMWARE: FROM OUR SMALL TOWNS IN MICHIGAN TO DC

Tuesday, June 28, 2022

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON INTELLIGENCE
AND COUNTERTERRORISM,
Lansing, MI.

The subcommittee met, pursuant to notice, at 11:01 a.m., at MSU Federal Credit Union, 3777 West Road, East Lansing, Michigan, Hon. Elissa Slotkin [Chairwoman of the Committee] presiding.

Present: Representatives Slotkin, Jackson Lee, and Demings.

Chairwoman SLOTKIN. The Subcommittee on Intelligence and Counterterrorism will come to order.

The subcommittee is meeting today on "Combatting Ransomware: From Our Small Towns in Michigan to Washington, DC".

Without objection, the Chair is authorized to declare the subcommittee in recess at any point.

Good morning, everybody. Thank you for joining us. I am happy to be here in my Congressional district in East Lansing, Michigan bringing Congress and the subcommittee that I chair to the people that I serve. The purpose of today's hearing is to bring some of the District of Columbia's best minds on cybersecurity to my district to detail the critical work that they are doing to keep ordinary Americans, like Michiganders, safe from an increasingly disruptive threat, and that threat is ransomware. Ransomware is a National security threat that has a direct impact on the lives of Michiganders.

Before I get into the details here, I just want to say we are live streaming. If you are behind our witnesses you are on camera. So let us keep your funny faces and pointing to a minimum since that will be recorded for posterity. We will have a number of Members from my subcommittee appearing virtually from their home districts, and I just really appreciate the opportunity to hold this here in Michigan and thank our leaders from Washington for flying in and doing this event.

So just a couple of definitions so we are all on the same page. A ransomware attack is defined as a digital form of traditional ransom, whereby computer systems, data, and electronic devices are held hostage by a criminal or group seeking a ransom payment in order for an organization to regain access to their own systems. They are often carried out by a criminal or criminal groups with the support or tacit approval of a state government, known as a

state actor. Think about criminals who are acting out of places like Russia and China. We have seen state actors and adversaries, Russia and China, but also North Korea and Iran, permissible territories. Other times these attacks are carried out by criminals purely for their own behalf. These are called non-state actors. According to a 2022 Cyber Threat Report by SonicWall, an internet cybersecurity company, ransomware attacks in the United States rose by 98 percent last year to record-high levels. I think in the State of Michigan we have heard from the State officials in our last hour that ransomware attacks in the State have doubled since last year. A separate report by the CyberEdge Group found that nearly two-thirds of ransomware victims actually went ahead and paid their ransom in order to regain access to their own systems and their own data. Often it is cheaper for a small or medium-size business or organization to pay the ransom than to pay an IT and cybersecurity company to regain all that access that they lost.

In Michigan alone we have heard from the State's chief information officer that hackers have tried more than 90 million times a day to get into the State servers. Let me say that again, that is 90 million times a day. Ransomware has become a kitchen-table issue for Michiganders. Often these are automated, right. It is not 90 million individuals, it is an automated process. But that is the number of times that there has been attempted infiltrations to our State every single day. Every Michigander in this room has their data held by the State. So that is our data.

Ransomware has become very much a kitchen table issue for us. It affects the people and organizations we rely on everyday, our schools, particularly our K–12 schools, our small businesses, our hospitals and third-party vendors that work with our hospitals, and other organizations, like our farmers, have been threatened and have even fallen victim to ransomware attacks.

I was really taken by this issue when I began as a Member of Congress. I was sworn in 2019 and I started making the rounds with our town supervisors, our mayors, our superintendents, folks who are in many cases very small rural communities and I expected—you know, I just said, what are you worried about, what are you concerned about, and I expected it to be about money and fixing the roads and some very concrete things. All of these folks started raising with me how concerned people were about cybersecurity for the 1,200 residents that they were responsible for.

It is an issue that I think I really—like lives in this Venn Diagram of National security issues and local issues. It is something that people are obviously rightly concerned about. We just came from a panel where we heard from town supervisors responsible for 1,200 people's data who were ransomed based on a phishing email for $40,000. A small community does not have $40,000 to just throw at this problem.

As a Nation, you might remember two high-profile kind-of newsworthy ransomware attacks last year. One was the Colonial Pipeline and one on the JBS Meat Company. These events really showed Americans how vulnerable we are, how our critical infrastructure is vulnerable to these attacks, and then how damaging the consequences can be. Many ransomware attacks have been

much more hyper-local though than these kind of high-profile events.

In Michigan's 8th district, which I represent, we have had a significant—as I said, a significant uptick in these attacks, which is why I have pulled together this field hearing. We have seen entire cities and townships targeted in these new attacks. Local governments have had to create entirely new websites, create new email addresses, buy new software to resolve these attacks, all at great cost and time and resources.

In a February *Detroit Free Press* article, Sgt. Matt McLalin, who investigates cyber attacks in the State Police's cyber command center, which is not far from here in Dimondale, Michigan, said local and county governments make up the majority of the center's victims. Every single week, he said, we are getting multiple reports of local governments that have been affected—every week. When an entire local government can be taken off-line by a cyber criminal operating across the world, we have a significant issue we need to address.

As I said, it is not just governments. Last fall I hosted the superintendents from my district. The K–12 superintendents came to Washington and I just sort-of on a whim said raise your hand if you have ever been a victim of a ransomware attack, and every single school superintendents hand went up. Some paid, some didn't. There they are trying to get the kids' identities, the kids' data.

We have seen schools come under direct attack in Walled Lake, Michigan; Monroe, Richmond, Michigan; and across the State. Last month, people may remember that classes at Kellogg Community College were canceled for 2 days as school officials noticed some issues with the computer systems related to a ransomware attack. Two years ago, Michigan State University, very close to here, was targeted by this increasingly prevalent type of attack, and it cost the university more than $1 million to recover.

Cyber criminals operate in permissive environments, like Russia and China, as we said. The governments at best turn a blind eye to these actors operating on their soil, at worst they know what they are doing and don't do anything about it. They have launched attacks, particularly for our kids, on their school records. These are useful for future hostage situations, ransomware situations because they presume that schools and parents will pay virtually any cost to shield their children from educational disruption.

As we have talked about, ransomware attacks have also disrupted hospital systems. The uptick on ransomware attacks during COVID was significant on our hospitals, but also on third-party vendors that do a lot of work with our hospitals. In addition, our gas pipelines, and, as the workers at JBS processing plant in Plainwell know, it has threatened literally our Nation's food supply and our farmers' livelihoods.

Further endangering our food supply, we have seen ransomware attacks directly targeting the manufacturers of agricultural equipment and the data they collect. Ransomware attacks are a threat to people from the smallest family farm to the biggest Fortune 500 companies, but it is the ordinary American, the farmer, the schoolteacher, the business owner, the parent, who bear the brunt of these attacks.

Just this past weekend, I heard from constituents in Brighton, Michigan, not far from here, that were fundraising for the owners of a local bookstore in Detroit which was hit by a cyber attack and was forced to personally cover over $35,000 in losses. That business, still fragile from COVID and the pandemic, is now facing the prospect of imminent closure as a result of this attack.

We know that our computer systems are complex, we know that small and medium-sized businesses, small and medium-sized governments are already stretched thin. They don't have the ability to hire fancy security firms to take care of everything for them. Not everyone can afford cybersecurity insurance, which is something I encourage all leaders to look into, and many are not able to hire a cyber specialist, an IT specialist on payroll to respond.

So this is why our hearing is so important today. We have designed the hearing to connect the average person with experts who can help them protect themselves. To our witnesses, people want to know where do they go when they are the victim of a ransomware attack. Literally, what is the 9–1–1 number that they call? Do they call the FBI? Do they call the State Police? Where should people turn the minute that they realize someone is trying to steal their data. We know that we have an increasing number of people who are just coming in for a normal day of work, they realize that their computer or their cash register is physically locked to them by hackers demanding large sums of money. We know that they are now—this is no longer sort-of asking that you drop a bag of cash at a designated location, the use of cryptocurrencies has been significantly on the rise. I have heard from constituents across the district that they feel like they are on the front lines of this threat and they do not know what their Government is doing to protect to them.

[The statement of Chairwoman Slotkin follows:]

STATEMENT OF CHAIRWOMAN ELISSA SLOTKIN

JUNE 28, 2022

I am happy to be here in my Congressional district in East Lansing, Michigan—bringing Congress and the subcommittee I chair to the people I serve. The purpose of today's hearing is to bring some of the District of Columbia's best minds on cybersecurity to my district to detail the critical work they are doing to keep ordinary Americans, like Michiganders, safe from an increasingly disruptive threat: Ransomware. Ransomware is a National security threat that has a direct impact on the lives of Michiganders.

First, some definitions: A ransomware attack is defined as a digital form of traditional ransom, whereby computer systems, data, and electronic devices are held hostage by a criminal or group seeking a ransom payment in order for an organization to regain access to its systems. They are often carried out by a criminal or criminal group operating with the support or tacit approval of a state government, known as a state actor. We have seen these state actors in adversaries like Russia, China, North Korea, and Iran. Other times they are carried out by criminals operating purely on their own behalf, known as non-state actors.

According to a 2022 Cyber Threat Report by SonicWall, an internet cybersecurity company, ransomware attacks in the United States rose by 98 percent last year to record-high levels. And a separate report by the CyberEdge group found that nearly two-thirds of ransomware victims paid the ransom to regain access to their systems and data. In Michigan alone, we have heard from the State's chief information officer that hackers try more than 90 million times a day to get into the State's servers. Let me say that again: 90 million times a day.

Ransomware has become a kitchen-table issue for Michiganders. It affects the people and organizations we rely on every day—as our schools, small businesses,

hospitals, and other organizations have been threatened by—and have even fallen victim to—ransomware attacks. When I first started as a Member of Congress, town supervisors, mayors, and local officials all surprised me by raising protecting data as something they were deeply concerned about. They were right to be concerned. From my first day as your Congresswoman, we have seen significant ransomware attacks against our critical infrastructure, local governments, entire hospital systems and school districts, all the way down to local mom-and-pop small businesses.

As a Nation, two high-profile ransomware attacks last year, one on the Colonial Pipeline and one on the JBS Meat Company, showed Americans how vulnerable our critical infrastructure can be to these attacks, and how damaging the consequences can be. But many ransomware attacks have been much more hyper-local to Michigan's 8th district, and that is why I am hosting this hearing here in East Lansing as opposed to in Washington. We have seen entire cities and townships targeted in these attacks. Local governments have had to create entire new websites, new email addresses, and new software to resolve the attack. All things which cost time and resources.

In a February *Detroit Free Press* article, Sgt. Matt McLalin, who investigates cyber attacks in the State Police's cyber command center, said local and county governments make up a lot of the center's victims. "Every single week we are getting multiple reports of local governments who have been affected," McLalin said. When an entire local government can be taken off-line by a cyber criminal operating across the world, we have a significant issue that needs to be addressed. It's not just governmental entities that have been affected, either.

Last fall, I met with school superintendents from across my Congressional district in my office in the District of Columbia. I asked them to raise their hands if they or their students had been hit by a ransomware attack—and every single hand in the room went up. We have seen schools come under attack in Walled Lake, Monroe, Richmond, and across the State. Just last month, classes at Kellogg Community College were canceled for 2 days as school officials noticed some issues with the computer systems related to a ransomware attack.

Two years ago, Michigan State University was targeted by this increasingly prevalent type of cyber attack, which cost the university more than $1 million to recover from. Cyber criminals operating in permissive environments like Russia and China have launched attacks aimed at holding our kids' educations, their school records, and their futures hostage because they presume that schools and parents will pay virtually any cost to shield children from educational disruptions.

As I alluded to earlier, it is not just our schools and our kids who are threatened. Ransomware attacks have disrupted hospital systems, gas pipelines, and—as the workers at JBS's processing plant in Plainwell know, it has threatened our Nation's food supply and our farmers' livelihoods. Further endangering our Nation's food supply, we have seen ransomware attacks targeting the manufacturers of agricultural equipment and the data they collect. Ransomware attacks are a threat to people from the smallest family farm to the biggest Fortune 500 company, but it is the ordinary American, the farmer, schoolteacher, and small business owner, who bears the brunt of these attacks.

Just this past weekend, I heard from constituents in Brighton that they were fundraising for the owners of a local bookstore in Detroit, which was hit by a cyber attack and was forced to personally cover over $35,000 in losses. That business, still fragile from the impacts of the pandemic, is now facing the prospect of imminent closure as a result of the attack. Computer systems are complex. Small businesses and local governments are already stretched thin, and not everyone can afford to have cyber insurance or an IT and/or cyber specialist on the payroll to respond.

That is why today's hearing is so important. We designed this hearing to help connect the average person with experts who can help them protect themselves. People want to know where to go when they are the victim of a ransomware attack. Do they call 9–1–1? Do they call the FBI? Do they call the State Police? Where should people turn when they realize someone is trying to steal data that they are responsible for protecting? People want to know what to do when they turn on their computer or cash register only to find out they are locked out by hackers demanding large sums of money, often in the form of cryptocurrencies, that they can't afford.

I have heard from constituents across many different industries about how concerned they are about the threat of ransomware. They feel like it's their business, their data, that is on the front lines facing this threat. They are especially concerned because they don't know what their Government is doing to protect them. I don't just want to draw attention to the problem: I want to use this hearing to discuss the ways that we are keeping Americans on the front lines of the ransomware threat and their data safe.

I am pleased to welcome witnesses who I know are working hard to combat ransomware and other cyber attacks every day, and who are eager to help us answer these questions. Visiting us from Washington are two representatives from the Department of Homeland Security (DHS)—Mr. Iranga Kahangama and Mr. Matt Hartman. Mr. Kahangama—who was integral to the Federal Government's response to the ransomware attacks on Colonial Pipeline and JBS Foods—is responsible for cyber and infrastructure protection strategic planning and analysis at DHS. At DHS's Cybersecurity and Infrastructure Security Agency or CISA, Mr. Hartman works on the front lines with partners at the State and local levels, as well as in the private sector, to defend against today's cyber threats and build security and resiliency.

On our second panel we will be hearing from one of our State's best cybersecurity experts—Mr. James C. Ellis, commander of Michigan State Police's Cyber Command Center. I look forward to hearing from our witnesses on the critical work they are doing to defend our local communities, our State, and our country, from the rising threat of ransomware and how they are partnering with the private sector to build resilience to ransomware attacks before they occur, because we know that the best way to defend against a ransomware attack is to take steps to protect yourself before an attack occurs.

Chairwoman SLOTKIN. So, with that, I am pleased to welcome our witnesses, who are working very hard on this threat and other cyber attacks and threats every day. We are eager to get to questions—I know we have members on screen visiting us from Washington.

Our two representatives from the Department of Homeland Security, Mr. Iranga Kahangama—can you say it for me so I say it right?

Mr. KAHANGAMA. Thank you. Kahangama.

Chairwoman SLOTKIN. Kahangama. And Mr. Matt Hartman. The former was integral to the Federal Government's response to the ransomware attacks on both Colonial Pipeline and JBS Foods. He is responsible for cyber and infrastructure protection strategic planning and analysis at the Department of Homeland Security.

Mr. Hartman, he is DHS's cybersecurity and infrastructure security—he is working on the front lines of CISA, which is the Cybersecurity and Infrastructure Security Agency. He partners with State and local officials, as well as in the private sector, to defend against today's cyber threats.

In our second panel, which will take place just after this, we will be hearing from one of our State's best cybersecurity experts, Mr. James Ellis, commander of Michigan State Police's Cyber Command Center.

I look forward to hearing from our witnesses on their critical work and what they are doing to defend our State and local officials, because we know that the best way to protect against a ransomware attack is to take steps to protect yourself before the attack actually occurs.

Before I formally welcome our panel of witnesses, Members on screen are reminded that the subcommittee will operate according go the guidelines laid out by the Chairman and Ranking Member of the full committee in their February 3, 2021 colloquy regarding remote procedures. Other Member statements may be submitted for the record.

[The statement of Chairman Thompson follows:]

STATEMENT OF CHAIRMAN BENNIE G. THOMPSON

JUNE 28, 2022

I am pleased that Intelligence and Counterterrorism Subcommittee Chairwoman Slotkin is holding this hearing on such a pressing issue, in her district with her constituents.

It is so important for communities to be heard, and hearings like these are a part of the Committee on Homeland Security's process to safeguard the American people and the Homeland from all threats, including cyber threats.

Cybersecurity is a topic that Chairwoman Slotkin has championed since she came to Congress, and she has worked tirelessly to keep the people of Michigan safe from cyber crime.

Given her extensive background in National security, she knows the threats we face whether at home, abroad, or in cyber space.

Her leadership led to new legislation that would provide cyber forensics training for State and local law enforcement and create an program to help ensure the Government is prepared for a major cyber attack.

Her work leading this subcommittee and as a Member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation has focused on emerging digital security issues that affect all of us—from the way we use our banks to the safety of our children's schools to how we can protect ourselves from criminals' latest techniques.

The internet is wired into nearly every part of our life—our homes, our cars, our schools, our businesses. It has become as important a utility as water, gas, and electricity.

But it has also become perhaps the greatest tool for criminal mischief and theft in history.

In what we call ransomware attacks, cyber criminals seize computer systems, data, and electronic devices with the expectation that victims will be willing to pay a ransom to regain access to their electronic systems.

Ransomware attacks have surged both in frequency and in the amount demanded by hackers. In 2020, an estimated 2,400 governments, hospitals, and school districts in the United States were victims of ransomware attacks, and the average payment was $312,493.

According to data from the Cybersecurity and Infrastructure Security Agency (CISA), reported losses continued to increase last year.

As ransomware tactics and techniques continue to evolve, we can expect more incidents and more losses unless we do something to address the root causes of the issue—both in Government and the private sector.

Thanks to the Biden administration, we have a National cyber director working to coordinate all of the Executive branch's work in cyber space.

The administration has also ensured that CISA is working across Government agencies to improve our collective defense and with the private sector to ensure it has the tools to detect, disrupt, and investigate cyber criminals.

In Congress, the Committee on Homeland Security has championed several critical pieces of legislation to combat the ransomware threat, including bills that:

- provide $1 billion in grants to State, local, Tribal, and territorial governments over the next 4 years to enhance their cybersecurity preparedness;
- make cyber incident reporting mandatory including the disclosure to CISA of ransom payments within 24 hours;
- direct CISA to conduct a study on K–12 cybersecurity and provide cybersecurity recommendations to K–12 educational institutions, which have faced numerous ransomware attacks in recent years; and
- authorize the Secret Service to continue training local, State, Tribal, and territorial law enforcement on cybersecurity investigations and responding to cyber incidents, including ransomware.

I am grateful for Chairwoman Slotkin's leadership and that of her committee colleagues on these important measures.

Although the Federal Government has made great strides in bolstering our defenses, as the threat of ransomware continues to disrupt many aspects of our daily lives, we must make sure that Americans know what resources are available to them—at both the Federal and State level.

It is imperative that the public knows how to keep themselves safe from ransomware attacks, and if they do fall victim to an attack, who they can reach out to for help.

If your car is stolen or your home is broken into, people know to call the police or 9–1–1—but when it comes to cyber theft, that common knowledge of who to call for help is not broadly known.

Today's witnesses—representatives from DHS and its cyber-focused component CISA, and the State of Michigan—are in a position to help us understand ransomware prevention best practices, and what to do and who to call when catastrophe strikes.

Again, I thank Subcommittee Chairwoman Slotkin for convening this hearing and for her leadership on this critical issue.

Chairwoman SLOTKIN. Without objection, Members not on the subcommittee shall be permitted to sit and question the witnesses.

Sorry for my Michiganders. This is a bunch of procedural things that are important in Congress.

All right. I now welcome our first panel of witnesses.

Without objection, the full witnesses' statements will be inserted into the record.

I now ask each witness to summarize his statement for 5 minutes, beginning, sir, with Mr. Kahangama. Please go ahead.

STATEMENT OF IRANGA KAHANGAMA, ASSISTANT SECRETARY FOR CYBER, INFRASTRUCTURE, RISK, AND RESILIENCE, OFFICE OF STRATEGY, POLICY, AND PLANS, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. KAHANGAMA. Thank you. Madam Chairwoman Slotkin, distinguished Members of the subcommittee, and other Members of Congress joining us today. Thank you for inviting me to testify about the Department of Homeland Security's efforts to combat ransomware.

On a personal note, this is my first time testifying. As the son of immigrants from Shri Lanka, it is an honor to be in front of you today.

With that, I recently passed the 1-month mark serving as the assistant secretary for cyber infrastructure, risk, and resilience at the Department of Homeland Security. My title, while long, is reflective of the holistic approach that the Department takes to ransomware and cybersecurity writ large. We are focused on critical infrastructure. We want to minimize the risk posed from cyber attacks, and we want to ensure the resilience of critical services that are provided to this country.

Today I will talk about the multi-pronged approach we are taking to combat ransomware and apply this framework to cybersecurity. As you mentioned, Chairwoman, ransomware attackers lock up our critical computer systems and then demand payment in order to regain access. They do not discriminate, they target large and small targets, whether it is large corporations, small and medium enterprises, hospitals, local governments, or schools. As you mentioned as well, often the cost of cleaning up an attack can be more expensive than paying the ransom itself, or to provide mitigating services beforehand.

I also want to acknowledge the downstream real-world impact that these have on our everyday services. As you mentioned, this happened with Colonial Pipeline where we had gas shortages, this happened to our food production when JBS was also attacked last year, and as you mentioned, a slew of attacks on Michigan itself.

These are real issues and I want to make clear that the Department recognizes these.

So today I want to talk a little bit about what the Department does before, during, and after a ransomware attacks.

So before an attack, the Cybersecurity and Infrastructure Security Agency, CISA, helps businesses and small business and critical infrastructure owners increase their ability to prevent a ransomware by rapidly sharing threat information and sharing cybersecurity best practices. I am honored to be here today with Matt, who will further provide information about CISA's role.

Last year Secretary Mayorkas conducted a 60-day sprint on combatting ransomware to shore up the Department's efforts on this case. As a result, we now have stopransomware.gov, which is a one-stop, holistic, centralized repository with all information that you need before and during an attack to help mitigate against ransomware incidents.

During an attack I want to highlight quickly the Department of Homeland Security's investigative agencies, which include the U.S. Secret Service and Homeland Security Investigations. These agencies work side-by-side with victims, international law enforcement, and domestic law enforcement to investigate and mitigate the threat posed by ransomware actors.

I appreciate your mention of cryptocurrency as the Department is rapidly increasing our ability to investigate cryptocurrency because it is the preferred payment method for ransomware actors. We are actively getting tools and learning how to track and trace cryptocurrencies so we can better disrupt and potentially claw back some of this money.

Of course, the Department also works in concert with the Department of Justice to arrest and indict these individuals when we can.

As you mentioned, Chairwoman, these actors are often in permissive environments that do not cooperate with us, including Russia. But that does not stop us from working with international partners to seize and track these funds and otherwise disrupt their criminal activity.

Finally, I want to hit on after an attack. I am excited to mention that DHS is now standing up the Cyber Safety Review Board, which is a unique combination of public-sector and private-sector individuals charged with reviewing major cyber attacks, including ransomware attacks, to provide recommendations of how to better our cybersecurity.

DHS remains committed to improving our Nation's cybersecurity, shoring up our defenses, improving the resiliency, and then holding actors accountable.

Chairwoman Slotkin, by holding these types of hearings, it is clear to us that you are committed to this issue. I also want to thank you for passing legislation such as the K–12 Cybersecurity Act. It is evident that you are a partner with us and we commend you for this. We look forward to working with you.

With that, I would like to thank the committee and I look forward to taking your questions.

[The joint prepared statement of Mr. Kahangama and Mr. Hartman follows:]

JOINT PREPARED STATEMENT OF IRANGA KAHANGAMA AND MATT HARTMAN

JUNE 28, 2022

INTRODUCTION

Chairwoman Slotkin, Ranking Member Pfluger, and distinguished Members of the subcommittee, thank you for inviting us to testify today regarding the continued threat of malicious cyber activities, specifically ransomware, and the constant risks posed to Americans, as well as to our businesses and other institutions. Our testimony today highlights the Department of Homeland Security's (DHS) efforts to counter these risks. These efforts are made in coordination with the Biden-Harris administration's counter ransomware initiatives, and our partners in Federal, State, local, Tribal, and territorial governments (SLTT), the private sector, and internationally.

Since Under Secretary Silvers and Executive Director Wales testified before your subcommittee last November, DHS has continued to combat the non-stop threat of cyber crime with several notable successes. However, these cyber threats continue to evolve, and we must therefore continue to evolve the methods that we use to investigate cyber-criminal activity and increase our Nation's resilience against future attacks. Our joint testimony today reinforces that our approach to cyber crime must be multi-pronged. We must pursue a comprehensive strategic approach that prioritizes close partnerships with law enforcement, both domestic and foreign, as well as the private sector, and combines our efforts to:

- disrupt cyber-criminal activity;
- increase resilience of entities and individuals to ransomware incidents;
- target those virtual currency exchanges and on-line dark marketplaces that enable the ransomware threat through obfuscation of illicit payments;
- investigate transnational cyber crime and organized criminal groups; and
- strengthen foreign law enforcement partner capacity through training and technical assistance.

Most cyber crime is transnational, including ransomware, with criminal activity moving seamlessly across borders. These crimes impact Americans in all 50 States, including Michigan's 8th Congressional district. For example, in 2016, the Lansing Board of Water and Light's administrative services were taken over by hackers as a result of a ransomware attack. Furthermore, in 2020, Michigan State University was a victim of a ransomware attack over Memorial Day. More broadly, DHS does successfully investigate cyber crimes in Michigan. Recently, U.S. Secret Service (Secret Service) agents from the Detroit Field Office successfully investigated a business email compromise case where they were able to return almost $5 million to the victim company.

DHS, in close partnership with the Federal Bureau of Investigation (FBI) and other law enforcement partners, prioritizes investigating cyber crimes, arresting those responsible, and seizing illicit funds and returning them to the victims. In addition, the Department engages the private and public sectors on how to increase their cyber resilience to fend off these attacks.

THE BIDEN-HARRIS ADMINISTRATION'S APPROACH TO FIGHTING RANSOMWARE

Ransomware threat actors' motives are clear—their goal is profit. These opportunistic criminals go after a wide array of victims—individuals, businesses, hospitals, police departments, and even municipal governments. These criminals encrypt valuable data in an attempt to force their victims to pay ransoms using virtual currencies, with no guarantee the criminal actors will provide a decryption key to restore the victims' files once the ransom is paid. Victims who choose not to pay are saddled with the cost- and labor-intensive burden of restoring their systems from backups and, increasingly, threatened with the public release of their stolen data by the criminal actors. The administration will not allow criminals to hold innocent American citizens and businesses hostage for ransom, or to extort victims with stolen private information, such as health records, without consequence.

The landscape of ransomware actors has undergone several shifts since the subcommittee's November 2021 hearing, driven in part by the Russian-Ukraine conflict. We observed some ransomware groups adopting political stances, such as the Conti ransomware group's initial pledge of support to Russia at the outset of the invasion of Ukraine. We also witnessed Conti become increasingly emboldened in their demands. For example, in May, Conti threatened to overthrow the Costa Rican government if ransoms were not paid, according to published reports. These criminal actors are resilient and resourceful. When victims stop agreeing to pay ransom, or

a ransomware operation is the subject of a law enforcement action, the actors move on to different victims and stand-up new ransomware groups.

Therefore, the Department must be equally resilient and resourceful, utilizing a whole-of-government counter-ransomware initiative with domestic and international partners to go after criminals while simultaneously promoting cybersecurity resilience across our critical infrastructure and American businesses. DHS's strategy is multi-pronged: Target and dismantle criminal ransomware organizations; target the digital asset ecosystem that criminals use to transfer illicit funds; and increase resilience in our Nation's critical infrastructure and public sector, through education and information sharing.

These partnerships continue to pay off in the fight against ransomware as demonstrated in March when an Estonian national was sentenced to 66 months in prison and $36 million in restitution for his role in exploiting stolen financial account information and use of ransomware.[1] The arrest and subsequent indictment were the result of the international partnership between the Secret Service, Latvian State Police, and Estonian Police.

Last year Secretary Mayorkas commenced a 60-day sprint as a call for action to tackle ransomware.[2] As a result, DHS, along with colleagues across the U.S. Government, launched "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. As of June 2022, StopRansomware.gov received over 280,000 visits.

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY EFFORTS ON RANSOMWARE

One of the Cybersecurity and Infrastructure Security Agency's (CISA) core functions is to foster 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 continues to take many proactive steps to prevent ransomware. These efforts include hundreds of engagements focused on cybersecurity and combatting ransomware. CISA routinely engages with SLTT partners, including events specifically for Governors and county leaders, as well as 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 and increasingly with foreign 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, which CISA provides through email and other subscription services.

Visibility and awareness also require information sharing and collaboration. In August 2021, CISA launched the Joint Cyber Defense Collaborative (JCDC) to lead the proactive 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 capabili-

---

[1] See, "Cybercriminal Connected to Multimillion Dollar Ransomware Attacks Sentenced for Online Fraud Schemes" at, *https://www.justice.gov/usao-edva/pr/cybercriminal-connected-multimillion-dollar-ransomware-attacks-sentenced-online-fraud.*

[2] 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.*

[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.*

ties necessary to truly make a difference for our Nation's cybersecurity posture. The JCDC brings 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 establishes a unique entity that can proactively provide visibility into a common operating picture of the threat environment through close partnership with the private sector and the Federal cyber ecosystem.

The Nation's security and resilience in the face of the ransomware threat relies on a collective, unified approach across the Federal Government that combines the full suite of relevant interagency authorities and capabilities. As designated in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), CISA will establish a Joint Ransomware Task Force to coordinate an on-going Nation-wide campaign against ransomware attacks. CISA and the FBI will serve as co-chairs of this Federal task force, which will organize and orchestrate the spectrum of U.S. Government activities to address the ransomware threat, from protection and mitigation to intelligence prioritization and disruption.

DHS INVESTIGATIVE EFFORTS TO COMBAT CYBER CRIME

The world's economy is rapidly changing and becoming more digitized. In partnership with international law enforcement partners, the Secret Service has achieved notable successes in combatting cyber-enabled financial crimes, including dismantling two early centralized virtual currency providers that supported extensive criminal activity: e-Gold Ltd.[5] and Liberty Reserve.[6] Additionally, in 2020, the Secret Service, with domestic and international partners, successfully investigated a Russia-based criminal scheme.[7] The investigation led to the seizure of millions in cryptocurrency and indictments of two Russian nationals.

Central to these successes is the global network of 44 Secret Service-led Cyber Fraud Task Forces (CFTFs). The mission of these CFTFs is to partner with SLTT and foreign law enforcement agencies, private and public sectors, and academia for information sharing and conducting joint investigations. The Secret Service also operates 19 international attaché offices around the world, partnering with the global law enforcement community to combat transnational financial crimes.

Participation in these task forces is bolstered through Secret Service-led law enforcement training programs at the National Computer Forensics Institute (NCFI). At NCFI, the Secret Service trains SLTT law enforcement personnel, prosecutors, and judges on preventing, mitigating, and responding to malicious cyber activities, including ransomware. Personnel who receive training serve as force multipliers complementing Secret Service CFTFs. Currently the NCFI's authorizing legislation (6 U.S.C. § 383) limits NCFI to training SLTT law enforcement officers. Congress is currently considering legislation to re-authorize NCFI, which could incorporate an authorization to train foreign partners.[8] In addition, Homeland Security Investigations (HSI) and Secret Service agents regularly participate in capacity-building workshops delivered through the U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN), a U.S. State Department Bureau for International Narcotics and Law Enforcement Affairs (INL)-funded initiative where digital forensics experts and long-term Federal agents deliver training and technical assistance to foreign partners that enables them to better cooperate with U.S. authorities, including on ransomware and criminal misuse of cryptocurrency investigations.

---

[5] See, U.S. Department of Justice: "Over $56.6 Million Forfeited In E-Gold Accounts Involved In Criminal Offenses," *https://www.justice.gov/usao-md/pr/over-566-million-forfeited-e-gold-accounts-involved-criminal-offenses;* Digital Currency Business E-Gold Indicted for Money Laundering and Illegal Money Transmitting, *https://www.justice.gov/archive/opa/pr/2007/April/07_crm_301.html.*

[6] See, U.S. Department of Justice press releases: "Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million Through His Digital Currency Business," *https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital;* "Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, and Seven of Its Principals and Employees for Allegedly Running A $6 Billion Money Laundering Scheme," *https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest.*

[7] See, "Russian Nationals Indicted for Conspiracy to Defraud Multiple Cryptocurrency Exchanges and Their Customers," *https://www.justice.gov/usao-ndca/pr/russian-nationals-indicted-conspiracy-defraud-multiple-cryptocurrency-exchanges-and;* "Treasury Sanctions Russian Cyber Actors for Virtual Currency Theft," *https://home.treasury.gov/news/press-releases/sm1123.*

[8] H.R. 7174—National Computer Forensics Institute Reauthorization Act of 2022. Available at: *https://www.congress.gov/bill/117th-congress/house-bill/7174.*

Today, the Secret Service coordinates, integrates, and shares information on ransomware cases through the FBI-led 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, including the FBI, State, Treasury, and other domestic and foreign partners. The Illicit Virtual Asset Information Notification system, a joint effort between multiple agencies, operates from the NCIJTF and, once fully operational, will enable increased partnership between Federal law enforcement and the private sector to detect and disrupt ransomware and other illicit virtual currency payment flows.

U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) has 80 offices in over 50 countries and works to combat cyber crime, including ransomware, through its Cyber Financial Section of the Financial Crimes Unit, which provides training to international partners and analytical assistance in tracing digital assets. In addition, HSI's Cyber Crimes Center (C3) has led numerous cyber-related trainings with foreign law enforcement partners. In 2020, HSI, working with the Departments of Justice and the Treasury, dismantled three terrorist financing cyber-enabled campaigns—involving al-Qaeda, Hamas's al-Qassam Brigades, and ISIS.[9] Since January 2020, HSI C3 conducted in-person and virtual training covering on-line investigations, dark web, and cryptocurrency investigations for law enforcement partners in over 20 countries. Some of this training was conducted in coordination with the HSI Financial Crimes Unit. For example, in May 2022, HSI C3 provided network intrusion investigations training to law enforcement officials in Panama.

Additionally, HSI initiated Operation Cyber Centurion, a cyber threat intelligence initiative that proactively detects vulnerabilities in critical infrastructure and works with victims to remediate the vulnerabilities before they are exploited. These vulnerabilities are often used to enable the theft of sensitive data or the disruption of a functioning system and are commonly used in ransomware attacks. Cyber Centurion is designed to significantly disrupt adversary plans to exploit the internet to subvert U.S. laws and threaten the economic integrity, public safety, and National security of the United States. The initiative is in alignment with CISA's priorities for the protection of critical infrastructure.

DHS is committed to strengthening the law enforcement capabilities of Secret Service, HSI, and other law enforcement partners to investigate all forms of cyber crime within our authorities and arrest those responsible.

INTERNATIONAL PARTNERSHIPS

Cyber criminals and nation-state actors will continue to view ransomware as an effective means to fund themselves and cause disruptive effects in critical infrastructure. It will take a global effort to stop them. To combat transnational cyber crime, including ransomware, both the Secret Service and HSI maintain close partnerships with a wide array of foreign law enforcement agencies. The Secret Service is the first U.S. law enforcement agency to have permanent representation at Europol with an attaché assigned to the Joint Cyber Crime Action Taskforce at Europol's European Cyber Crime Centre.

In March, DHS hosted the Cross-Border Crime Forum with our Canadian partners to make our nations safer and committed to working together to combat ransomware, strengthen security and resilience of critical infrastructure against these threats, as well as increase reporting of ransomware incidents. In May, DHS leadership attended the Ottawa 5 meeting in London, where discussions focused on combatting ransomware.

Last fall, the United States hosted a Counter-Ransomware Initiative meeting with international partners from more than 30 countries. Delegates discussed common challenges, approaches, and opportunities to advance international cooperation to achieve shared goals. DHS serves as the lead for the United States on the sub-group focused on resilience. DHS, together with the Departments of Justice, State, and Treasury, also recently participated in the initial meeting of the U.S.-E.U. Ransomware Working Group.

The Department continues to work together with like-minded foreign partners to target, identify, and prosecute cyber criminals, disrupt their malicious IT infrastructure, and shut down financial networks used to launder illicit proceeds. In April 2022, the Secret Service announced that an international operation, organized by Europol and conducted in partnership with the FBI, resulted in the seizure of the

[9] See, "Global disruption of 3 terror finance cyber-enabled campaigns," *Global disruption of 3 terror finance cyber-enabled campaigns|ICE.*

RaidForums website—a popular marketplace for cyber criminals to purchase and sell hacked data. This successful outcome was the result of combined efforts between the Secret Service, other Federal agencies, as well as international partners, including the United Kingdom's National Crime Agency.[10]

CONCLUSION

The Department commends Congress for passing the fiscal year 2022 Omnibus Appropriations bill, which passed in March and included the language from CIRCIA. In addition, we greatly appreciate Congress' continued support for the cyber training of SLLT law enforcement. Centers such as the NCFI provide critical cyber investigation skills and tools to our partners needed to prevent, mitigate, and respond to cyber incidents.

DHS is committed to countering the cyber crimes targeting our country, our citizens, and our partners around the world. 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 ensure the success of DHS's multi-pronged mission to increase cyber resilience, disrupt the ransomware ecosystem, and hold accountable those who commit these crimes. Thank you again for the opportunity to testify and we look forward to your questions.

Chairwoman SLOTKIN. Thank you for your testimony.

I now recognize Mr. Hartman to summarize his statement for 5 minutes.

STATEMENT OF MATT HARTMAN, DEPUTY EXECUTIVE ASSISTANT DIRECTOR FOR CYBERSECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. HARTMAN. Excellent. Thank you. Chairwoman Slotkin and Members of the committee, thank you for the opportunity to testify today on behalf of the Cybersecurity and Infrastructure Security Agency, or CISA, to discuss our efforts to elevate America's security and resilience against ransomware attacks.

As the Nation's cyber defense agency, CISA leads the National effort to understand, manage, and reduce risk to the digital and physical infrastructure that Americans rely on every hour of every day.

Here in Michigan, and in every State across the country, ransomware and the threat of cyber attack are top-of-mind concerns to schools, to hospitals, to businesses large and small, and to so many other organizations. That is why it is important that we empower organizations and Americans to help us raise the cybersecurity baseline.

The administration's approach to countering ransomware is focused on bolstering resilience. Strengthening resilience to withstand ransomware attacks is arguably the most difficult element of our collective efforts. I am pleased to testify today on CISA's efforts to help tackle this problem.

Building resilience requires a long-term investment in people, processes, and technology. Every organization that wants to avoid being the victim of ransomware must continuously invest in the practices that will keep their customers, their systems, and their data secured.

The question that we need to ask ourselves is what can we do right now to truly have an impact. I will point to two things. First,

[10] See, "U.S. Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator," *https://www.justice.gov/usao-edva/pr/us-leads-seizure-one-world-s-largest-hacker-forums-and-arrests-administrator*.

we must give organizations tools and guidance to increase their security and resilience. This is why CISA works every day to raise awareness and to promote basic cyber hygiene across tens of thousands of businesses and government agencies throughout our country. Organizations need to raise their cybersecurity standards and the guidance that CISA provides is meant to provide real-time actionable information to help them do so. For you, that means regularly update your software, think before you click, avoid suspicious links and phishing emails, use strong passwords, and, most importantly, implement multi-factor authentication. Adding a second factor for log-in makes you 99 percent less likely to be hacked.

Second, we need to partner with the American people, organizations in both the public and private sectors to identify threats and vulnerabilities, to develop guidance, to conduct outreach, and to ensure that everyone has the information that they need to make educated cyber risk management decisions.

CISA is uniquely positioned to build and strengthen partnerships with the private sector and with State, local, Tribal, and territorial government organizations. A central element of our ability to partner with you here in Michigan and across the country is CISA's growing presence outside of Washington, DC. CISA has cybersecurity advisors now in nearly every State, including two here in Michigan, to provide boots on the ground help to organizations of all sizes to address the growing threat of cyber attack. Additionally, CISA's Joint Cyber Defense Collaborative, or JCDC, was launched to drive partnership between the Federal Government and private-sector companies who possess tremendous visibility into domestic networks to help us identify emerging threats and to provide timely and actionable cybersecurity guidance to reduce the risk of attack for everyone.

A great example of this guidance is CISA's Shields Up messaging campaign which we launched in the lead-up to the Russian invasion of Ukraine. Through more than 100 engagements with different critical infrastructure sectors and organizations, we showed organizations, regardless of size, how to strengthen their cybersecurity and resilience. With information from the intelligence community and the private sector, we use *CISA.gov/shields-up* to provide evolving threat information to serve as the hub for up-to-date technical guidance to reduce risk. To date, this is one of CISA's most visited pages on *CISA.gov*.

Additionally, last summer we launched *stopransomware.gov,* a collaborative U.S. Government resource to help public and private organizations tackle ransomware. The web page has had more than 830,000 views and the ransomware readiness assessment tool that has been downloaded and is available on that site has been downloaded roughly 15,000 times. Please help us get the message out that this tool is there for organizations across America.

We are working closely with Federal partners to stand up the Joint Ransomware Task Force, a new tool Congress gave us, which is the governing body to combat ransomware attacks from mitigation and protection to intelligence prioritization and disruption. CISA is proud to serve as co-chair of the Task Force, along with the FBI.

CISA has been leading this whole-of-Nation effort with partners across the Government and private sector, but now more than ever we need everyone, including the business and government right here in Michigan to work with us to reduce this threat because it impacts us all.

Thank you again for the opportunity to appear before you. I look forward to your questions.

Chairwoman SLOTKIN. Thank you for your testimony.

I thank all the witnesses.

I will remind the subcommittee that we will each have 5 minute for questions to question the panel.

I now recognize myself for questions.

Thank you for your testimony. You know, Mr. Kahangama, we have, as I look around the room, some farmers in the room and I know that you responded to both the attacks on the Colonial Pipeline and the JBS meat processing facility. Can you describe some of the specific lessons learned? I mean these are big organizations who, you know—we certainly had the head of Colonial Pipeline come and testify in front of us and talk about some of the security vulnerabilities that they had in a very large organization, but if you are a farmer in the State of Michigan, you are dependent on some of these large organizations to get your product out to market. Can you talk about some of the lessons learned from those attacks?

Mr. KAHANGAMA. Thank you for the question, Chairwoman. Absolutely.

I think one of the lessons learned is that no matter how big an organization you are, the smallest cyber vulnerability can be quite damaging. I think it is also important to understand the connection between regular systems that you may use for H.R. or doing paychecks versus all the operational components. I think in both of those instances with Colonial and JBS we saw relatively small attacks that targeted like a payroll system and then out of an abundance of caution the entire enterprise shut down. So I think we are all susceptible to the lowest common denominator of cybersecurity that is provided.

The other thing that I want to mention is that ransomware attackers are quite vigilant and they are looking for businesses and services that they know will want to pay. I believe the FBI put out an advisory in the wake of JBS not just mentioning that vulnerabilities exist, but that ransomware actors can and will look for opportune times in cyclical seasons, right. With the agricultural and food process and grain production for instance, there are certain times of year where crops may be more valuable and you would be more likely to pay because you need to plan the seed or grow the crops and things like that.

So ransomware actors are actively looking at your business time line and looking to target you at opportune times when they know you may be more willing to pay.

So I think being vigilant 24/7 365 days a year, including patching those vulnerabilities, were some of the big takeaways I took from that.

Chairwoman SLOTKIN. Great. Thank you for that.

Mr. Hartman, a few years ago one of our local infrastructure authorities ended up paying $25,000 in ransom to unlock their internal communications systems. Responding to that attack, in addition, cost them $2.4 million. Luckily the attack did not disrupt our—literally our power grid or our water distribution networks as they had insurance and provided protection against network disruption. There are many organizations who do not have that insurance, who do not have that cushion. We heard in our previous roundtable from a local town supervisor who represents I think less than 2,000 residents where the ransomware was $40,000, right. It is just—and luckily they had insurance, or else that would have been borne by a local government that just cannot afford it.

So how can you help—you know, the JBS and the Colonial Pipeline, they are very wealthy companies that can hire their own IT folks. Tell us what you can do for our smallest businesses and who do they call the minute they walk into work and there is a problem?

Mr. HARTMAN. Thank you for the question, Chairwoman.

You know, there are four things that I will point to that every organization, large or small, should consider. This is as applicable to farmers and schools as it is to the Colonial Pipelines and the JBS Foods.

The first I touched on in my opening remarks, which is implement multi-factor authentication. This is something that every person, every organization should do. A password as a sole identifier is no longer sufficient. But implementing a second layer, whether that is a fingerprint, facial recognition, a text message, email, again, you are reducing your risk of being a victim of ransomware by 99 percent.

To your point, Chairwoman, with 90 million attempts a day targeting state systems, we know that this is broad indiscriminate and opportunistic scanning and targeting of all of our domestic critical infrastructure.

The second piece is extraordinarily important. To your point about not having the resources to pay, it is critical to maintain offline encrypted back-ups and to periodically and regularly test that you are able to recover to these back-ups so if your data is encrypted you are not forced with the decision of whether to pay or not.

Third, all organizations should develop an instant response plan; they should test this plan frequently. It is absolutely paramount that cybersecurity starts at the top of the organization, at the board level, at the CEO level. These plans need to exist. I can speak from experience that organizations who are working to develop incident response plans on the fly are generally not particularly successful.

Finally, and to your last question, report your incidents to CISA. This is important for two reasons. First, if we do not know, we can't help. Secondarily, if we do not know the tactics that are being used, if we do not know the infrastructure that is being used, we cannot share that information in anonymized fashion more broadly to protect the community. So get to know your local cybersecurity advisors from CISA, get to know your FBI field offices. The real important thing is that you contact one of us and then on the back

end we will work within the Department of Homeland Security, with our peers at the FBI, to make sure that we can provide all of the assistance of the Federal Government.

Chairwoman SLOTKIN. Thank you for that.

The Chair will now recognize other Members for questions they may wish to ask the witnesses.

In accordance with the guidelines laid out by the Chairman and Ranking Member on their February 3, 2021 colloquy, I will recognize Members in order of seniority, alternating between Majority and Minority where possible. Members participating virtually are also reminded to unmute themselves when recognized for questioning.

The Chair recognizes for 5 minutes the gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Madam Chair, thank you so very much for having me this—having this hearing in particular. Again, thank you for your enormous leadership. As I have served on this committee, it is clear that the importance of both the Homeland Security Committee and the Department of Homeland Security, and what you have done in this particular committee is to bring this knowledge both to our local communities, but as well as to listen to them.

Today we have the opportunity to listen in Michigan and understand the growing cyber threats that impact businesses, local communities, and of course school and other organizations.

This is crucial and I am looking forward to the continued testimony about the pay. "Ransomware bosses make $90,000 annually." Just to read it, "If crime doesn't pay, Russian ransomware bosses wouldn't know it. The average Russian ransomware boss makes $90,000 a year, or 13 times the average income for citizens in the country." I ask unanimous consent to introduce that into the record.

Chairwoman SLOTKIN. So ordered.

[The information follows:]

SPOTLIGHT ON SECURITY

Crime Pays: Ransomware Bosses Make $90K Annually

http://www.technewsworld.com/story/83603.html, By John P. Mello Jr., June 14, 2016 5 o'clock AM PT

If crime doesn't pay, Russian ransomware bosses wouldn't know it.

The average Russian ransomware boss makes US$90,000 a year—or 13 times the average income for citizens in the country who stick to the "straight and narrow," according to a recent Flashpoint study.

What does a ransomware honcho do for those rubles? Basically, the job calls for supporting and maintaining the malware.

"The software has to be constantly updated so that antivirus systems won't recognize it as malware," explained Vitali Kremez, a cybercrime intelligence analyst with Flashpoint.

"It's not a situation where you provide the malware and sit back on a couch waiting for your payments. You have to work on it on a daily basis," he told TechNewsWorld. "The boss controls the source code for the malware."

Ransomware as a Service

The malware model is evolving, according to the Flashpoint study, which focuses on the Russian ransomware scene.

"A new form of ransomware has been developed that is in effect 'Ransomware as a Service' (RaaS)," notes the report. It "enables 'affiliates' to obtain a piece of ransomware from a crime boss and distribute it to victims as these affiliates wish."

That's a departure from the past, when ransomware was available only to criminals willing to make a hefty upfront payment for the malware—$2,000 to rent or $5,000 to buy. That began to change last November, Kremez noted.

"We started to see developers considering giving their malware free of charge to criminals and keeping 40 to 50 percent of each ransomware payment made," he said.

The new business model has lowered the barriers to getting into the business. It is not particularly hard for newcomers to start spreading ransomware quickly. They can attack corporations and individuals through botnet installs, email and social media phishing campaigns, compromised dedicated servers and file-sharing websites.

"It used to be a one-on-one business," Kremez said. "At this stage, it's all automated. We see marketplaces. We see services on the dark web where you deposit your money and buy what you have to buy without any direct communication with the seller."

Malicious Infrastructure Growing

More evidence of the popularity of ransomware is evident in Infoblox's latest quarterly report on malicious infrastructure building globally.

To measure that kind of activity world-wide, Infoblox has created a threat index. Upon its launch in the first quarter of 2013, the threat index was 76. During this year's first quarter, the index reached it's highest point ever: 137.

Activity related to ransomware has fueled the index's rise.

"While exploit kits remain a major threat, this latest jump was driven in large part by a 35X increase in creation of domains for ransom ware over the previous quarter, which in turn drove an increase of 290 percent in the overall malware category," the report states.

The activity of malware kit developers is another indicator of ransomware's attractiveness to criminals. Kits are used to infect devices with a variety of malware programs.

"A number of exploit kits and threat actor gangs behind them have started adding ransomware to their repertoire over the last few months," said Sean Tierney, director of cyber intelligence at Infoblox.

"These are gangs that were using their kits to deliver other kinds of malware," he told TechNewsWorld, that "have either started including or switched entirely to ransomware."

It's likely that the ransomware market will level off as security software makers get better at detecting it and consumers get smarter about avoiding it, suggested Tierney.

"Then the market will become saturated," he said, "and the return won't be able to support the amount of activity going on.

Expanding 2FA

Two-factor authentication, which requires both something you have and something you know in order to access an account, has proven to be a good way to thwart data thieves. One problem with the technology, though, is that it isn't easy for many rank-and-file developers to deploy. One authentication company aims to change that with a recently launched program.

Centrify actually goes beyond 2FA to include single sign-in—which allows the use of a single set of credentials to log into multiple accounts—along with password reset and access control of a device. Under the program, developers can plug into those features through Centrify system APis.

"Developers who are building an application from a great idea aren't necessarily expert in security," said Chris Webber, security strategist at Centrify.

"We can give that to them," he told TechNews World.

"They can take advantage of all the user management and multifactor authentication that Centrify's built, so they don't have to learn about that world and can concentrate on their great idea," Webber pointed out. "It's more and more critical that we need to figure out how to put two-factor auth everywhere, because passwords alone are just not a great way to do authentication anymore."

Breach Diary

- May 30. Troy Hunt, who maintains the data breach awareness portal Have I Been Pwned, advises his subscribers that information on 65 million Tumblr accounts is being offered for sale on the dark web.
- May 30. Twitter account of Katy Perry breached and her 89 million followers sent tweets filled with profanity and slurs, TechCrunch reports.
- May 31. MySpace announces it has reset the passwords of all accounts created prior to June 11, 2014, due to a data breach.

- May 31. A Federal district court in Pheonix, Arizona, rules that insurance provider Chubb does not have to reimburse P.F. Chang under a cybersecurity policy for payments to credit card processors connected to a 2014 data breach.
- June 1. U.S. Federal Reserve detected more than 50 breaches between 2011 and 2015, including several incidents described in internal documents as espionage, Reuters reports.
- June 1. Medical information of thousands of NFL players is at risk after backback [sic] containing the data was stolen from an athletic trainer's car, Deadspin reports.
- June 1. FBI alerts public that extortion attempts are being made against victims whose personal information has been compromised in recent large data breaches. Extortionists are threatening to make victim's personal informtion public if not paid two to five bitcoins.
- June 1. TeamViewer reports it experienced a service outage due to a DDoS attack, but its systems were not breached by hackers.
- June 2. Medical records of some 40,491 customers of the Stamford Podiatry Group in Connecticut impacted due to a system intrusion, HealthIT Security reports.
- June 2. 2015 payroll tax data of employees of Verify Health Systems in California at risk after an employee was duped by a phishing scam, SC Magazine reports.

Ms. JACKSON LEE. In addition, "Houston Rockets targeted in ransomware attack", and the idea of it is their network is attacked, a sports organization.

[The information follows:]

HOUSTON ROCKETS TARGETED IN RANSOMWARE ATTACK, REPORTS SAY

Channel 13 Eyewitness News, Thursday, April 15, 2021

https://abc13.com/houston-rockets-cyberattack-nba-ransomware-who-cyber-attacked-attack-against-team/10517049/

HOUSTON, Texas (KTRK).—The Houston Rockets insist a recent ransomware attack against their network has not impacted the NBA team's operations, even though the party claiming responsibility says the club's internal business data was stolen, according to reports.

As reported by Bloomberg News and Reuters on Wednesday, a Rockets spokesperson said "it appears that the unknown actors attempted to install ransomware on certain internal systems . . . our internal security tools prevented ransomware from being installed except for a few systems that have not impacted our operations."

Bloomberg reports the hacking group called "Babuk" claims on its dark web page to have stolen 500 gigabytes of the team's data, including contracts, non-disclosure agreements and financial data. Babuk is reportedly threatening to publish that information if the team declines to pay.

The Rockets spokesperson acknowledged the claims but wouldn't comment further.

The team added the attack hasn't affected its ability to "take care of our fans, employees, and players."

Still, it appears the Rockets are among many businesses rolled into a recent spike in ransomware attacks. Check Point Research reports a 50 percent increase in the daily average of ransomware attack attempts in the second half of 2020 compared to the first half.

In Houston, significant entities including Memorial Hermann and Texas Children's Hospital have reported previous breaches.

Ms. JACKSON LEE. So to Mr. Hartman and Mr. Kahangama, let me ask you these questions please, and if both of you would answer.

We understand that Michigan, along with other State laws, does not require attorneys general to be notified of data breaches and they may in fact receive their information by media. I would be interested in CISA's status of publishing rules about mandatory incident reporting.

Many of you know that I have introduced legislation on zero-day activities and it is important that we protect our local communities from that.

Finally, let me understand more on the work that has been done by the administration, the hard work, to prevent ransomware attacks from Russia and to find out whether or not we have been able to see a decrease or what has happened with respect to the ransomware attacks from Russia, particularly as they intrude into local communities.

If you would start first, assistant secretary of policy, and then CISA. Both of you can answer in the time that I have left.

Mr. KAHANGAMA. Thank you, Congresswoman. Happy to answer those questions.

I will start with the last one first and speak a little bit about the Russian engagement.

The U.S. Government, you know, did engage with the Russians early last year to address the threat of ransomware. President Biden has acknowledged it as a National security threat. While we did see some arrests occur, the Russian invasion of Ukraine has changed the calculus. We have seen some ransomware actors declare loyalties or sympathies with the Russian government. We have also seen them in Costa Rica target specifically governments. I think whether or not the Russians take action, we are willing to unilaterally continue the fight against these actors. I think you have seen that through the administration's approach, which has evolved to not just indictments and arrests, but taking back money, disrupting the financial say of the cryptocurrency ecosystem as well as using Treasury sanctions to disrupt cryptocurrency services that are essentially laundering a lot of these funds. We are going to continue to take that fight to them, including law enforcement actions, along with inter-agency partners.

Then to the Congresswoman's first question, I want to turn it over to CISA.

Mr. HARTMAN. Thanks, Iranga, and thank you, Congresswoman.

Ms. JACKSON LEE. Thank you. And your rules, potential timing that they may be coming out.

Thank you.

Mr. HARTMAN. Absolutely. Thank you, Congresswoman.

With respect to the Cyber Incident Reporting for Critical Infrastructure Act that was recently passed by Congress, thank you. This is going to be monumental in terms of the Federal Government being able to understand what is happening from a ransomware and a broader cybersecurity perspective and cyber incident perspective, as well as take action as a U.S. Government to deter future attacks.

With respect to the implementation of the legislation, we are in the process of a very thorough and rigorous rulemaking process. We intend to really find the sweet spot in implementation between, you know, defining the types of incidents that need to be reported to the Federal Government and when to allow victim organizations to focus on restoring their systems and data, but also in sufficient time providing the information to the Federal Government so we can limit the impact of a potential campaign and help the broader community.

Within 24 months we intend to have—be complete with rulemaking and work with our partners at the Federal Bureau of Investigation to make sure that when CISA receives information about ransomware or other cybersecurity incidents from all sectors, that we are quickly sharing that information back with the FBI, with the Sector Risk Management Agency from any of the 16 sectors, and with appropriate State and local authorities so that we as a community can take action to combat this problem.

Ms. JACKSON LEE. Thank you.

I yield back.

Chairwoman SLOTKIN. Great. Thank you.

The Chair recognizes for 5 minutes, the gentlewoman from Florida, Mrs. Demings.

Mrs. DEMINGS. Yes, good morning, everyone. Chairwoman Slotkin, thank you so very much for this very important and timely hearing. Regardless of what part of the country we are in, this is a topic that is certainly important to all of us. We all represent larger cities and smaller cities and towns and rural areas, so thank you so very much for this.

I do not want to just slaughter the witness' name. I will take a stab at it. Mr. Kahangama—if that is wrong, please forgive me—you talked earlier about the cost of sometimes cleaning up the attack can be less than the—paying the ransom itself. As we try to get different organizations to, you know, take steps to fight against cyber crimes, establish plans and programs, do you find that that in and of itself is just a major deterrent to actually developing plans? Or is that something that you have, you know, actually looked into?

Mr. KAHANGAMA. Thank you for the question, Congresswoman.

I think the more preventative measures that are taken in the front end, the cheaper your overall experience is going to be within cybersecurity. I think it is always going to be a little bit more expensive to deal with the long tail of issues that your organization needs to deal with afterwards. You have to constantly——

Mrs. DEMINGS. Do you find that organizations are open to that though? That they understand that as opposed to just wanting to move on quickly, pay the ransom, let us move on quickly? Or are they really open to what you were saying and practicing that policy?

Mr. KAHANGAMA. Thank you.

I think they are open. I think it is a matter of us educating them. I want to also bring in my colleague from CISA, who is on the ground with a lot of these companies as well. But I do think they are open and unfortunately a lot of them discover after it is a little too late.

But I want to defer to Matt as well.

Mrs. DEMINGS. Thank you.

Mr. HARTMAN. Absolutely. Thank you for the question, Congresswoman.

To my colleague's point, I think that organizations do understand and they are increasingly open to that concept. But to his other point, they may not know where to begin. This is where it is increasingly important that the Federal Government, that CISA real-

ly help organizations prioritize their scarce resources and prioritize their scarce time.

I will start by flagging that perhaps the most important element of what we can do as CISA is our regional cybersecurity forces. So for folks in Michigan, for folks across the country, if you do not know your CISA regional cybersecurity expert, get to know them. They can help you understand the services that we have to offer, they can help you prioritize where to begin. One service that we offer for free is a ransomware readiness assessment that all organizations can use and our CSAs across the 50 States can help organizations exercise these plans. We also have a suite of services that we call our "cyber hygiene services" that are scalable and available to all organizations in the country. These focus on the most common vectors of ransomware. So we have remote phishing campaign assessments, we have web application scanning, vulnerability scanning. You can sign up for this service for free, you can come to *stopransomware.gov* or *CISA.gov,* you can contact your local advisor and you will be emailed in an automated report every week illustrating the biggest challenges that you have and really helping your organization, no matter how small or how large, begin to prioritize vulnerabilities that you are closing, an investment that you are making in cybersecurity.

Mrs. DEMINGS. Sounds like you have certainly taken the steps to make sure that you have the resources and services available to organizations. But I guess I am more interested in are they taking advantage of it? What steps have you taken to make sure they are aware of it?

You talked earlier about all organizations should have an incident response plan. From a regional standpoint—and you can pick any region that you want to—have you seen great success with organizations developing that response plan? Or is there still a lot more work to do?

Mr. HARTMAN. Good question, Congresswoman.

We are seeing increased success by the day, but there remains work to do. There are so many organizations in this country, many of which, the vast majority of which are owned and operated by the private sector that are vital to our Nation's critical infrastructure, to our National critical functions. We are out there every day, we are increasing our field presence every day, we are increasing our resources every day. But it is through hearings like this, it is through every opportunity that we can to come to the local jurisdictions, come to States to talk about what we are doing every day to educate on the resources that are available that will really begin to, you know, make a big difference across the country.

Mrs. DEMINGS. Thank you so much.

Madam Chair, I yield back.

Thank you.

Chairwoman SLOTKIN. Thank you.

I just want to pile on to Congresswoman Demings' question because I think even for the businesses and organizations here in Michigan in the room, they did not know that they could go to their local CISA representatives and basically get—I mean we won't call it an audit, but an assessment of their cyber health. I just can't make it any more clear how important I think that is, that if you

wait until the moment when you have an attack and you are not prepared, you have already kind-of lost half the battle. I think one of the things that is most useful is, one, getting that assessment and then testing it a little bit. You know, and I always repeat the story that we did at the Pentagon. When I was at the Pentagon they realized that they had some vulnerabilities with phishing, right, with like even senior three- and four-star generals clicking on a phishing link that we got into our email system. So we did our own fake phishing email and you could identify exactly which individuals in your organization clicked on that link and created a vulnerability. Surprise, surprise, it tended to be some of our most senior folks. So they took it a lot more seriously.

So I think getting sort-of an assessment of your organization is—it is free, it is the most valuable thing that CISA can do and they are here based in Michigan. Your counterparts are here based in Michigan.

We will now move to a second round.

Mr. Kahangama, earlier this month I chaired a hearing on cryptocurrencies and I think a lot of people are just—it is a really new field for a lot of people. They don't understand how cryptocurrency works. We know that terrorist and criminal organizations can exploit these products and services to advance their plots. Just last week, in response to the large number of criminal acts involving cryptocurrency, an organization called Chainalysis announced a new service focused on crypto incident response to help their clients' response when they have been asked to pay in cryptocurrencies.

Can you just, for the lay person, explain how this works and kind-of the frequency with which cryptocurrency is now like the currency of choice for these attacks?

Mr. KAHANGAMA. Thank you for the question, Chairwoman.

Wholeheartedly agree. It is almost exclusively cryptocurrency at this point. These are digital assets, digital tokens that are created and then transacted on-line. The issue that we are having with them is that they exist in ungoverned space, right, whereas when you are taking cash or your paycheck to the bank and depositing it, those institutions are required to have Know Your Customer laws and identify who you are, identify where the money is going. There are laws that if your transactions are over a certain amount of money, that that gets flagged to the Federal Government for suspicious activity reporting. All these types of checks and balances are on those transactions. Those don't exist with cryptocurrency. They are generated through a number of technical means and then operate in an unregulated environment.

From a law enforcement perspective, from our Secret Service and other investigators, it can be difficult because on top of the anonymity that exists with the cryptocurrency, there are additional services that can mix up all those transactions and obfuscate them further, so it becomes even more difficult to track and trace. So without kind-of proper regulation and oversight of a lot of these cryptocurrencies, we are going to continue to be challenged by them.

Chairwoman SLOTKIN. So we heard from a local official in our first roundtable this morning who talked about how, you know,

after the attack they went back and this malicious actor had like gone in for a minute and tested their systems, then a couple of weeks later went in for 12 minutes, tested the system, and then was able to access it and ransom for $40,000, asking the local officials to translate regular cash into cryptocurrency in sending that over. The criminals did it as a matter of course and they sort-of used volume as the way to get as much money as possible.

So it is not that there is a live human being I guess on the other end of that attack, that they are just like farming out all these attacks at the same time.

Can you explain that a little bit, about how these like ransomware farms are working in places, particularly overseas?

Mr. KAHANGAMA. Sure. Thank you for the question, Chairwoman.

I think it is appropriate to liken a ransomware organization almost to a modern-day mob or mafia. It is very large structures. There is something called ransomware as a service, which you break up a ransomware attack into different parts, right. There is initial access, there is deploying malware, there is getting the money. These are kits that you can literally buy on-line. As a result, anyone with very basic technical knowledge can become a ransomware operator unfortunately.

So with this lowest common denominator environment you have a proliferation of individuals who are seeking to conduct these attacks. The fact is that they like to do onesies and twosies in very small increments in order to not go on the radar, right, to be undercover a little bit.

So I think you have ransomware actors growing in terms of their sophistication, but at the same time the tools they have are becoming quite basic. So you have very low-level people conducting these attacks at a much higher frequency with a wide availability of these tools. So it is a growing issue.

Chairwoman SLOTKIN. Yes. We heard that these bad actors, are sort-of cuing their ransom dollar amounts to the size of the organization and what they think they can produce and even sort-of looking at the revenue of a business, looking at, you know, for our schools who have to be transparent about the amount of money that they handle, that that helps them gauge what to charge in a ransomware attack. I thought that was disturbing that they sort-of know their victim and key the cost of something that they could reasonably or of some form afford so that they actually pay it.

Mr. KAHANGAMA. That is a real reality. These people kind-of want anything they can get. They will do their market research on victims, who can afford it, they will look at people who have cyber insurance to see if they are more susceptible to paying it. They also look to opportune times when they know they can't—they lock your system up and it is a week to graduation, so someone may be more interested in paying, and things like that. I wholeheartedly agree.

Chairwoman SLOTKIN. Thank you.

The Chair recognizes for 5 minutes the gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Let me again emphasize my appreciation for this hearing.

I can't emphasize enough the cruciality of the question of local governments, local businesses. I would like both witnesses to really

focus on, one, the importance of that individual assessment, but more importantly to say to local entities, you are not immune from international ransomware attacks. That is why this is such an important hearing. Frankly, we should probably work to do this across the Nation of the many Members' districts where people really think that they may be immune.

How often should a small government, a tax office, a small business, do their own self-analysis or their self-audit, as the theme has been, frankly? As you are beginning, Mr. Hartman, under our new legislation to develop the process for mandatory incident reporting, there needs to be some interim way that our local communities can be heard or that our State governments can be notified. What would be—first question is the importance of recognizing that no entity, no hamlet is immune, no village, no city, no sports organization, no school district. Then, second, what should they be doing in the interim as you are proposing? Both can answer this question. The protocols for mandatory incident reporting. Many of us have had these large entities in our districts and we are reminded of the Pipeline incident.

But I would appreciate you responding to those two questions.

Mr. HARTMAN. Thank you very much for the questions, Congresswoman.

First, to absolutely reiterate your point, no organization in this country is immune from cyber attack emanating from foreign nations. With that said, no organization in this country should feel that they have to take on this challenge alone. That is why we are here as CISA, to work together, to work collaboratively every day, to make sure that all organizations have the information that they need to make educated risk management decisions and to strengthen their own cybersecurity and their own resilience.

With respect to your second question on the frequency of how organizations should continue to self-evaluate or self-assess their cybersecurity, again, it really depends. There are many elements of the cybersecurity program, like knowing your exposed vulnerabilities that are externally facing, so that are available to—that are facing the internet and can be accessed by anyone across the world. Knowing your prevalence of external-facing known vulnerabilities, particularly those that we know our adversaries are exploiting. CISA recently developed a catalog of known exploited vulnerabilities that is available to all organizations to help them prioritize their vulnerability management programs.

With respect to what organizations should do in the interim, it is very simple. While there is no rule in place today, organizations can voluntarily report cyber incidents to report@CISA.gov. You can also report it to your field advisor or to the FBI. It is extremely important, again, that all organizations are aware of the services that the field support from CISA offers, from assessments to evaluations of your own organization's cybersecurity risk to education and encouragement of best practices to building cybersecurity communities of interest to quite frankly listening to our stakeholders' concerns, to their challenges, and to their requirements so we can work with Congress to increase the services that we provide to all.

Thank you.

Mr. KAHANGAMA. Congresswoman, I would just add in the remaining time that we also have cyber fraud task forces through the Secret Service. There are 44 of them globally. I believe there is one in Houston, Texas as well. These are joint task forces with local and State officials, as well as Federal law enforcement, who work together to share information rapidly and are also a resource for sharing information to and with the public on ransomware attacks.

Ms. JACKSON LEE. Well, let me conclude, in the time—my clock has gotten away from me—but let me just simply say that this is a frightening experience when you experience a ransomware attack. From our experience with Colonial Pipeline, I want to emphasize through this hearing, do not accept this attack alone. There are resources. Do not I think engage in ransom without engaging the government that is here and ready to serve and to help you.

So I hope as we proceed we will see a new protocol, but more importantly, don't experience or suffer the impact alone. I hope this hearing evidences that, that we are here to provide the assistance necessary.

Madam Chair, thank you so very much.

With that, I yield back.

Chairwoman SLOTKIN. Thank you, Congresswoman.

I just want to again foot stomp that for our local businesses, our superintendents, our school officials, our farmers, making an appointment to speak with our local officials who do cybersecurity in the State of Michigan ahead of need is always better than having that first call be an emergency. I think what is not always known is that groups can just—you know, if you are from a chamber of commerce and you get together with your group and you want to have a meeting with these folks, if they are available, they want to meet with the public. So folks should avail themselves of that.

With that, the Chair recognizes for 5 minutes the gentlewoman from Florida, Mrs. Demings.

Mrs. DEMINGS. Again, thank you so much, Chairwoman Slotkin.

Just again, and I know we have spent a considerable amount of time on this, but it is so very critical, having grown up in a rural part of Florida, I just think about the unique challenges that our smaller cities or smaller towns, our rural areas have, No. 1, in receiving the information, but then also if they receive the information, really being able to implement recommendations due to lack of resources. So, you know, any additional steps or assistance that we can give as Members of Congress to make sure that the information is passed on, you know, from the largest of municipalities down to the smallest, please, to both of our witnesses, let us know how we can be of greater assistance there. We have to be proactive as opposed to reactive, as has been said numerous times, to these type of attacks.

I would like to hear from both of our witnesses about—and if you want to respond to that at all, that is fine—but some of the challenges in recruiting a ready-for-the-moment work force. We know that many of our Federal agencies are experiencing challenges in recruitment and development. I also know that the advisory committee's recommendation was to prioritize, you know, our work force issues so that we could be more competitive with the private sector.

So if both of our witnesses would just speak for just a moment on how are we doing with our work force.

Mr. KAHANGAMA. Thank you for the question, Congresswoman.

We agree there is a cyber work force shortage in this country. It is an issue that the Government faces, the private sector, State and local communities writ large. I think it is important that we focus, you know, not just on traditional educational pathways as well. Having a diverse background in terms of what you may or may not have experienced, what kind of certifications you have are important.

For our secretary, Secretary Mayorkas, this is a high priority as well. He conducted a sprint on cybersecurity work force hiring last year as well. Happy to report on that front that we had a 60-day sprint last summer. I believe at least 500 job offers were given out in cybersecurity for the Department. That was the largest single hiring event we had so far and we have at least 300 of those onboard so far. But I also want to share with Matt because I know that CISA is doing a lot of great work in this space.

Mr. HARTMAN. Thanks, Iranga, and thank you very much for the question, Chairwoman.

Up front, you know, this is a challenge for all of our organizations. It is a challenge in the Federal Government. We understand it is a challenge in State, local, Tribal, and territorial governments, and it is a challenge in the private sector right now to fill critical cybersecurity jobs.

Within CISA we are taking this extraordinarily seriously. Similar to the Secretary, Director Easterly has really gone on record to say that we need to not only rapidly close our own cybersecurity work force gaps at CISA so we can better serve our communities, but we need to use this opportunity to close a significant diversity gap within our own organization. Director Easterly has gone on record stating that by 2030 we need to make sure that at CISA 50 percent of our cybersecurity jobs are occupied by women. That would be up from about 25 percent today. So that is a very strong goal and we are taking that signal and we understand that we really need to use this opportunity where we have a handful—a number of vacancies at CISA due to rapid growth in recent years, to make sure that our work force of tomorrow represents the diversity of our Nation.

With respect to specific actions, we are leveraging all of the tools at our disposal, including the Cyber Talent Management System, which we appreciate the support for. We have a hiring event tomorrow actually, a virtual hiring even where we are looking to bring in at least—I am targeting about 100 candidates tomorrow to be selected for the vacancies within my organization within CISA so we can really continue to do better for all of you, so we can provide the guidance that all organizations can leverage.

Back to your initial question, Congresswoman, the faster that we hire, the more diversity that we bring into our thought at CISA, the better the guidance that we can bring out to our diverse communities, to our diverse States.

Mrs. DEMINGS. Great. Well, again, thank you so very much to both of you for the work that you are doing.

Madam Chair, I yield back.

Thank you.

Chairwoman SLOTKIN. Thank you, Congresswoman.

I want to thank our panel for appearing today. Our witnesses flew out in order to join us here. Thank you for answering our questions and bringing the Federal perspective here to Michigan.

In just a second we are going to transition to our second panel. Mr. James Ellis, he's the cyber section commander at the Michigan Cyber Command Center at Michigan State Police Headquarters, and brings this sort-of into an even more local perspective.

Without objection, the subcommittee will recess for 5 minutes so that we can change the panel and folks can take a quick break. For our live-stream folks, we will be back after a brief break and come back and hear our second panel.

Thank you very much to our witnesses for making the effort to come out here.

Have a good one.

[Recess.]

Chairwoman SLOTKIN. Welcome back, everyone. Thank you for sticking with us and for those on the live stream, we will now continue to the second portion of our panel today.

Our witness today is Mr. James C. Ellis. He is detective first lieutenant and cyber section commander at the Michigan Cyber Command Center for the Michigan State Police. That is in Dimondale, Michigan.

Mr. Ellis leads a cyber team of over 100 Michigan State Police members located throughout Michigan and oversees the Michigan Cyber Command Center, or MC3, Computer Crimes Unit, and the Michigan Region of the Internet Crimes Against Children Task Force.

Mr. Ellis' team at the Michigan State Police Cyber specializes in high-tech criminal investigations of all types, proactive cyber investigations involving the on-line exploitation of children, and evidential forensic data recovery services.

Detective First Lieutenant Ellis is a 28-year member of the Michigan State Police and holds multiple cybersecurity industry certifications in addition to his Bachelor of Science degree.

I also want to note that we had planned for a second witness, but due to COVID unfortunately our second witness was unable to make it today. We wish her well.

Without objection, the written testimony of Ms. Laura Clark, chief information officer of Michigan's Department of Technology, Management, and Budget, will be inserted officially into the record.

[The prepared statement of Ms. Clark follows:]

PREPARED STATEMENT OF LAURA CLARK

JUNE 28, 2022

Thank you, Congresswoman Slotkin, for inviting me to speak today on the subject of cybersecurity. As the chief information officer and chief security officer for the State of Michigan, I appreciate the opportunity for me to discuss with the Members of this committee the steps we are taking to secure our State.

CYBERSECURITY IN THE STATE OF MICHIGAN

In the State of Michigan, information technology (IT) and cybersecurity are centralized under the Department of Technology, Management, and Budget (DTMB). Several years ago, both cybersecurity and physical security were consolidated into

one area within DTMB known as Cybersecurity and Infrastructure Protection (CIP), which serves to secure the State and ensure the safety of the Executive branch. Within CIP, there are several groups that provide external outreach to keep those within Michigan safe, further strengthening the cyber environment:

- Michigan Cyber Security (MCS) manages information security for the State of Michigan. The Michigan Security Operations Center has several advanced security capabilities including threat hunting, incident response, digital forensics, and vulnerability management. The Risk, Compliance, and Delivery division assumes responsibility for the process, tool, and governance of security process plans and security awareness campaigns, and developing and enforcing security policies, standards, and procedures for the enterprise to follow. Security architects establish the target security and infrastructure architecture for security platforms, implementing frameworks and solutions to keep the enterprise secure.
- Michigan Cyber Civilian Corps capitalizes on the cybersecurity talent within Michigan to allow qualified technical cybersecurity professionals and experts to volunteer to respond to cybersecurity events and incidents on behalf of the State. By participating in the MiC3, members receive training to further increase their knowledge and skills and can participate in State-wide exercises, encouraging outreach between cybersecurity-minded individuals.
- Michigan Cyber Partners is a collaboration between divisions at the State of Michigan, local public entities across the State, Federal agencies, and National non-profits to work to strengthen and improve cybersecurity. Michigan Cyber Partners offers members the ability to share information and threat intelligence with one another, participate in State-wide exercises and formal annual training offered to local government and K–12, and offers program oversight for risk assessments and Federal grant programs.
- Michigan Secure is a first-of-its-kind, free State-wide mobile protection app for residents. Michigan Secure protects users from cyber criminals and potential dangers encountered in the digital mobile world. The app was designed with security and privacy at the forefront, collecting no user data or identifying information.
- Resident Tooling is an effort to elevate the existing State of Michigan cybersecurity website and provide various cybersecurity information and resources to equip residents with the knowledge they need to stay safe in the on-line world.

Additionally, organizations that DTMB partners with who have a critical role in maintaining a safe cyber environment across the State:

- Michigan Cyber Command Center (MC3) is housed within the Michigan State Police and coordinates cybersecurity-related activities as they pertain to emergencies and computer-based crimes, extending beyond government information to reach all of Michigan.
- National Guard has both Air and Army National Guard Units with cybersecurity capabilities, in which the State of Michigan works closely with the Guard to formalize the process of working together in the event of a cyber emergency.

To aid in the distribution of roles and responsibilities between MCS, MC3, and the National Guard, the State of Michigan has developed the Michigan Cyber Disruption Response Plan (CDRP). The CDRP details chain of command, responsibilities, and processes for escalation, serving as a plan to weaken the unknown and panic that often coincides with major incidents. To guarantee the effectiveness of the CDRP, involved agencies and partners participate in workshops to review the CDRP and relative responsibilities and engage in functional exercises that simulate various scenarios and incidents that advance in severity. In completing workshops and exercises, we can ensure that proper action and best course of action is taken in the event of a cyber incident.

The Cyber Disruption Response Team (CDRT) is currently being utilized as a result of on-going geopolitical situations, with several meetings to share the latest information occurring throughout the week that allows for the consolidation of information sharing and the streamlining of sources while offering efficiency in the consumption of information. The frequent communications have established clear triggers for the escalation of an incident and the implementation of primary and alternative communications plans through various platforms, including Microsoft Teams and HSIN.

FEDERAL ASSISTANCE TO THE STATE

Consistent working relationships within the State of Michigan between MCS, MC3, and the National Guard are crucial to defend the State's digital landscape, and the relationships we have with our Federal partners is also highly valuable.

The Department of Homeland Security's (DHS) Cyber and Infrastructure Security Agency (CISA) has brought forth several resources to assist in securing Michigan's landscape. Through our CISA cybersecurity liaison, we have a direct line of communication with DHS who offers the Federal perspective to assist in the decision-making process. We also have contact with the Federal Bureau of Investigations (FBI), which shares valuable information on cybersecurity events and topics to ensure we protect the State.

Additionally, the Infrastructure Investment and Jobs Act (IIJA) will be a major asset to cybersecurity efforts across the State to further secure the digital environment. With an estimated $24 million being allotted to Michigan over the course of 4 years, Michigan's digital landscape has the ability to be transformed. The State of Michigan has developed a cybersecurity planning committee comprised of cybersecurity experts in various fields and locations to assist in determining how the distribution and use of the allocation of funds would best strengthen the digital ecosystem across the State while securing the State and local governments, schools, and entities. Federal partners have been directly engaged in the information sharing surrounding IIJA, participating the meetings and communications plans to provide key insight on the funding and state of cybersecurity.

BEYOND THE STATE: SECURING THE DIGITAL ECOSYSTEM

The transformation of the digital environment has resulted in Federal, State, and local governments being intertwined and relying upon with information sharing to help secure the ecosystem. Levels of government interact daily to improve the digital security of various environments while encountering challenges faced by human and financial resource shortages. The diversity in resources within these levels of government needs to be considered when addressing improvements to Michigan's digital landscape. For example, Michigan has 83 counties, 276 cities, 257 villages, and 1,240 townships. The population and available resources vary between these areas, resulting in an array of differing needs, improvements, and focuses across each level.

To assist in addressing the needs of local public entities and further secure Michigan's digital ecosystem, the State of Michigan, through the Michigan Cyber Partners program, offers the ability to contract for an independent cybersecurity risk assessment. The multiple pre-qualified vendors offered by the State were selected through a competitive request for proposal process, allowing entities to work with a vendor to complete assessment, planning, and coaching services to further strengthen their digital environments.

The findings of the risk assessments will assist in establishing a baseline for Michigan's plan for IIJA cyber implementation, indicating which improvements should be made with the funding to enhance security levels. Recommendations of transitioning to .gov domains for county and local governments, implementing multi-factor authentication across entities, and offering security awareness programs are being considered to further secure the State's digital environment. These items, among other options, are associated with the funds appropriated through IIJA, offering opportunities for entities beyond what they may typically have the funds to support. This reveals the need for sustainable funding post IIJA, as recipients may select a short-term benefit rather than long-term due to lack of budgetary funds. Securing the ecosystem needs to be a continuous effort, not a short-term solution.

The State of Michigan's external outreach programs also assist in securing the ecosystem. The MiC3 and Michigan Cyber Partners programs encourage discussion among cyber professionals, government entities, and educators, equipping them with the community and information needed to further secure the digital environment. The Michigan Secure app ensures that residents are kept safe on their mobile devices, and the elevation of the external cybersecurity website provides residents with additional resources to keep them safe on-line. The Michigan Cyber Summit, an annual cybersecurity conference available to the public, also offers valuable information sharing through its speakers and panels, providing insight on current cybersecurity topics from various perspectives.

The digital ecosystem is dependent upon governments, entities, and citizens working together to maintain and secure a safe environment. I would like to thank the Legislature and Governor Whitmer for their bipartisan support and recognition of the importance of cybersecurity, as well as the members of our Michigan Congressional delegation who continue to make cybersecurity a priority, especially those who voted for IIJA and its funding support. With new threats emerging each day, it is crucial that we strive to protect our State. The State of Michigan greatly appreciates the Members of this committee highlighting the importance of the digital eco-

system, and we look forward to continuing to work with you to secure it and protect residents.

Mr. Ellis, I would ask you to first kind-of lay the framework. We are now getting to the portion of our hearing that is really focused on our Michigan viewers, our Michigan businesses, our Michigan organizations and how they specifically can be helped within the State. We heard from the Federal level and I would ask you to now to summarize your statement for 5 minutes please.

STATEMENT OF JAMES C. ELLIS, DETECTIVE FIRST LIEUTENANT AND CYBER SECTION COMMANDER, MICHIGAN CYBER COMMAND CENTER, MICHIGAN STATE POLICE

Mr. ELLIS. Thank you subcommittee Chairwoman Slotkin and the Members of the committee for gathering us here today, or in this case just myself at this point in time, on the issue that is of crucial importance to the State of Michigan and the Nation.

My name is Detective First Lieutenant Jim Ellis and I am the cyber commander of the Michigan State Police, Michigan Cyber Command Center, or MC3, as we call it.

The first thing I want to do is establish a foundation of how the MSP fits into cybersecurity as a State Police law enforcement organization with Michigan critical infrastructure, the public, and our close partners. MSP Cyber is a full-service criminal investigation section. Members are in the field pursuing active investigations from initiation to prosecution, arrest, and court testimony. MSP Cyber supports all MSP troopers and field members, along with the other 580+ law enforcement agencies in the State and others nationally requiring investigative assistance as cyber crime has no State line boundaries.

It is becoming very difficult to name a crime that does not involve technology of some kind that may contain digital evidence supporting that crime. Some of the services, just to give you an example, that we perform, obviously criminal investigations. Thousands of cases per year. Last year alone we assisted over 340 police agencies in Michigan. This includes network intrusions, breaches of Michigan businesses, the forensic recovery of digital evidence used for prosecution or acquittal, hundreds of search warrants annually, receiving and seizing thousands of devices typically per month that require forensic examination, provide community outreach and presentations covering cyber security, provide law enforcement with education and training regarding cybersecurity, collaborate with critical infrastructure regarding information sharing and best practices. We conduct cyber assessments for public and private industry businesses as well.

MSP Cyber, as you stated, is comprised of over 100 highly specialized members consisting of uniformed and civilian investigators. Cyber analysts, members from within the Michigan Department of Corrections, Michigan National Guard as full-time positions, and we all have members on the FBI Cyber Task Force, Homeland Security Investigations, Dark Web Task Force, and I can't leave out our two cyber-trained canine dogs, and many other support staff.

MSP overall consists of three units. We have the Computer Crimes Unit, known as CCU, which was created by necessity in 1999 when computer technology was being used in the commission

of crimes and the internet was thought to be a fad. The CCU investigates high-technology crimes and provides digital forensics data recovery, as stated.

The Internet Crimes Against Children Task Force. The ICAC, as we call it, is a collection of State, local, and Federal partners concentrating on child sexually abusive material, known as CSAM, and exploitation crimes, including child trafficking and investigations.

The third unit is the Michigan Cyber Command Center, which has been established to coordinate cyber crime incident response and investigative network information system-based crimes affecting Michigan. The MC3 is a leading resource for cybersecurity, cyber crime awareness and prevention, and network-related investigations. Investigations do include network intrusions, breaches, unlawful access, hacking, theft, and exfiltration of data, extortion and cyber terrorism, as is surrounding this today with cryptocurrency and other forms of malware. We also do malware identification, research, and analysis. Information sharing of breach notification, development, and dissemination of various intelligence products are also pushed out by the MC3 for Michigan businesses and citizens.

Including in our State partnerships within the State of Michigan government ecosystem, MSP Cyber, DTMB's Michigan Cyber Security, Michigan Air and Army National Guard, and others have a long-standing collaborative partnership with the purpose of ensuring the cybersecurity posture through prevention and response within the State of Michigan. Together we have been a role model for many other States and major cities across the United States who hope to replicate what we have done to assist in better securing the State. Michigan is one of the first States to create a State-level cyber disruption and response plan that has been used across the Nation as a template. Together we have partnered to develop and fuel many initiatives. That includes the Michigan Cyber Civilian Corps, know as the MiC3, Michigan Secure App that you can put on your mobile devices, the Cyber Partners Group, the Chief Security Officer Cabinet Meetings, and many others bringing everyone together simply to discuss cyber best practices and to reinforce information sharing.

We participate together in multiple cyber exercises, workshops, and presentations every year and involve Federal partners, critical infrastructure, and Government to assist in ensuring the cybersecurity of our water treatment plants, energy-producing facilities, financial institutions, academia, election systems, and other. On almost a daily basis we are sharing cyber-related information among the many partnerships that have been developed to ensure the best possible cybersecurity protections are in place.

Thank you for your time and this opportunity to share our experiences in Michigan and I look forward to addressing any questions you may have for me.

[The prepared statement of Mr. Ellis follows:]

PREPARED STATEMENT OF JAMES C. ELLIS

JUNE 28, 2022

Thank you, Subcommittee Chairwoman Slotkin, Congresswoman Jackson Lee, and the Members of this committee for gathering us here today to discuss this issue of crucial importance to the State of Michigan and the Nation. My name is Detective First Lieutenant James Ellis, and I am the commander of the Michigan Command Center within the Michigan State Police.

MICHIGAN STATE POLICE—CYBER SECTION

The Michigan State Police (MSP) Cyber Section, referred to as "MSP Cyber", is within the Intelligence Operations Division of the MSP and works in conjunction with the Michigan Intelligence Operations Center. Let me establish a foundation of how the MSP fits into cybersecurity as a State police law enforcement organization, with Michigan critical infrastructure, the public, and our close partners, the Department of Technology Management and Budget (DTMB) and the Michigan National Guard.

MSP Cyber is a full-service criminal investigation section responsible for investigations spanning the entire criminal file class hierarchy. MSP Cyber members are in the field pursuing active investigations from initiation and investigation to prosecution, arrest, and court testimony. MSP Cyber supports all MSP troopers and field members along with the other 580+ law enforcement agencies in the State and others nationally requiring cyber-related investigative assistance, as cyber crime has no State line boundaries. As our case load continues to increase year after year, it is becoming very difficult to name a crime that does not involve technology of some kind that may contain digital evidence supporting that crime.

Services performed by MSP Cyber include but are not limited to:

- Criminal investigations both originating and assisting in an undercover capacity—over 4,000 cases per year, assisting over 340 police agencies last year in Michigan
- The forensic recovery of digital evidence used for prosecution or acquittal
- Street-level and electronic surveillance
- Search warrants—over 400 hundred per year; both administrative and on-scene with physical device and digital evidence seizures
- Often receiving and seizing over 1,000 devices per month for forensic examination and recovery of digital evidence
- Provide expert courtroom testimony
- Provide community outreach and presentations covering all cyber/computer-related topics from prevention and awareness to incident response and cybersecurity best practices
- Provide law enforcement with cyber, computer crime, and digital evidence-related education and training
- Collaborate with critical infrastructure regarding information sharing and incident response
- Conduct cyber assessments for public and private industry/businesses
- Conduct criminal investigations involving the sexual exploitation and trafficking of children including the rescuing of children from sexual predators
- Investigate hundreds of cybersecurity-related network intrusions and breaches of Michigan businesses annually
- Sourcing new initiatives for the MSP and the State of Michigan related to data security, privacy, policy, and compliance
- Develop and submit legislative language and provide testimony for new and modified Michigan laws regarding cybersecurity.

We work collaboratively with all other law enforcement, public/private sectors, critical infrastructure, small/medium/large businesses, local, State, and national government organizations, local community groups, and citizens.

MSP Cyber is comprised of over 100 highly-trained and specialized members consisting of both uniformed detective troopers and sergeants, officers, cyber analysts, dark web analysts, digital forensic analysts, incident response teams, an FBI Cyber Task Force member, a Homeland Security Investigations (HSI) Dark Web Task Force member, Michigan Department of Corrections staff members, National Guard members, two cyber-trained K9 dogs, and many other support staff.

MSP CYBER ORGANIZATIONAL UNITS

MSP Cyber consists of three organizational units that work in collaboration and provide overlapping services that include the Computer Crimes Unit (CCU), the

Internet Crimes Against Children (ICAC) Task Force, and the Michigan Cyber Command Center (MC3).

Computer Crimes Unit (CCU)

Created by necessity in 1999 when computer technology was being used in the commission of crimes and the internet was thought by some to be a fad. The CCU is the premier State-wide leader in responding to and investigating high-technology crimes and providing digital forensic evidentiary data recovery assistance to local, county, and State law enforcement agencies. The CCU operates multiple digital forensic offices throughout Michigan for the purposes of digital forensic examination and analysis.

Internet Crimes Against Children Task Force (ICAC)

The ICAC Task Force is a collection of State, local, and Federal partners concentrating on child sexually abusive material (CSAM) and child sexual exploitation and trafficking investigations. MSP Cyber has the responsibility to train local law enforcement in the proper acquisition and examination of digital forensic evidence. Currently, over 50 Federal, State, and local law enforcement agencies supply dedicated officers to investigate ICAC cases, with most of them working directly out of MSP Cyber offices. MSP Cyber also receives all Michigan cyber tip investigations that are reported by the National Center for Missing and Exploited Children (NCMEC) located in Washington, DC. In 2021, the MSP Cyber received 11,416 cyber tips, averaging almost 1,000 investigations per month.

Michigan Cyber Command Center (MC3)

Established in 2013 by necessity to coordinate cyber crime incident response and investigate the proliferation of networked information system-based crimes affecting Michigan. The MC3 is a leading resource for cybersecurity, cyber crime awareness and prevention, and cyber-related network intrusion criminal investigations for critical infrastructure; Federal, State, and local government entities; other public and private sectors, and citizens of the State of Michigan.

- Primary investigations include:
  - Network intrusions and breaches; unlawful access, hacking, theft, and exfiltration of data
  - Extortion and Cyberterrorism
  - Dark Web and Cryptocurrency.
- Malware identification, research, analysis, origin, indicators of compromise for awareness/prevention
- Provide cybersecurity assessments, industry best practices, and recommendations
- Information sharing; breach notifications, development, and dissemination of various intelligence products; podcasts, presentations, media events, news releases
- Partnerships and collaborations—national, State, and local; FBI, HSI, USSS, DHS, and others.

MICHIGAN CYBER—STATE PARTNERSHIPS

MSP Cyber, DTMB's Michigan Cyber Security (MCS), Michigan Air and Army National Guard, and many others along the way have had a long-standing collaborative partnership of almost 10 years with the purpose of ensuring the cybersecurity posture through prevention and response within the State of Michigan. Together we have been a role model for many other States and major cities across the United States, who hope to replicate what we have done as a State when it comes to securing the State through prevention and response, not only within State government, but in addition to the many relationships we have created within our public and private partnerships across Michigan.

Michigan was one of the first States to create a State-level Cyber Disruption and Response Plan that contains the framework and details related to responsibilities and roles that covers how to manage a State-level cyber disruption, that has been used across the Nation as a template, since the original version was finalized almost a decade ago. We have partnered to develop and fuel many initiatives that include the Michigan Cyber Civilian Corps (MiC3), Michigan Secure App, Cyber Partners Group, chief security officer (CSO) cabinet meetings, and many more, bringing everyone together to discuss cyber and reinforce information sharing, creating multiple plans, exercising those plans, education, awareness, prevention, compliance, knowing who to contact.

We participate together in multiple cyber exercises, workshops, symposiums, and presentations, every year and involve Federal partners DHS, FBI, others within

Michigan from critical infrastructure sectors including health care, finance, energy, water, education, and Government to assist in ensuring the cybersecurity of our water treatment plants, energy-producing facilities, financial institutions, academia information systems, election systems, and others. On almost a daily basis we are sharing cyber threat detection, prevention, awareness, and recovery information among the many partnerships that have been developed to ensure the best possible cybersecurity protections are in place.

Thank you for your time and this opportunity to share our experiences in Michigan, and I look forward to addressing any questions you may have for me.

Chairwoman SLOTKIN. Great. I thank the witness for his testimony.

I will remind the subcommittee that we will each have 5 minutes to question the panel.

I now recognize myself for questions.

So tell me, Mr. Ellis, you know I think one of the things we talked about earlier this morning was kind-of that moment, that moment that a superintendent or a business owner or a local elected walks into his or her office and realizes that they have been completely locked out of their data, that they are a victim, and they have that moment of panic, right. They are being ransomed, they are being threatened. If they are seated in the State of Michigan, what should they do? Quite literally, what is the—how do they figure out who to call and then walk us through what the process will be like once they call.

Mr. ELLIS. Sure. The most important thing is to call. They can certainly call the Michigan Cyber Command Center at the Michigan State Police. They can call DHS. But that is probably the No. 1 question we get is, who do we call? Really it comes down to call whoever you are comfortable with on the law enforcement side because when it comes to the investigation in law enforcement your case is going to get to the agency that it needs to get to.

Within the State Police, obviously, as I mentioned, we have liaisons with Federal partners, including FBI, Secret Service, Homeland Security. So they are going to be involved regardless. But quite frankly they need to make a call. It really doesn't matter which agency they call. Obviously we tell them to call us.

Once they do, we will attempt to understand what has occurred at their location, how many devices, what they think they are seeing, whether it is malware, ransomware, or the type of malware, if they have back-ups, that type of thing. We will kind-of do an evaluation or an assessment on the phone. We will get other partners involved if we need to. What is crucial for us is we will typically instruct them how they can best provide evidence to us, whether that is us coming on scene if we need to image a system. Because one of the things we want to do, even though we are talking cyber and we cannot always prosecute on cyber crime because actors are in other places or they are anonymous, is we want to get those indicators of compromise of how this started on their systems so we can take that, research it, and then push it back out for prevention and awareness to all the other businesses to help them establish protections so they don't have to go through the same thing this business just went through.

Chairwoman SLOTKIN. Yes, I think that is something that when I have talked to local businesses they are like, look, I sort-of handled it myself. I said, you know, the trends and the similarities be-

tween these attacks can help, you know, another business from having to go through the same thing and that if law enforcement isn't aware of what has gone on in your case, they can't help another business, they can't identify those bigger trends.

Then are you—what—how do you handle when someone says they are asking me for a $40,000 ransom payment, should I pay it, what should I do? How do you advise individuals and companies how to respond?

Mr. ELLIS. Yes. We typically will tell them not to pay because it simply empowers or emboldens the bad actors to continue with their ransomware. You know, we will obviously prepare them to help establish if they are able to restore data, if they have come to the point where they actually have an encrypted data. A lot of times we will get calls when they see some instances of ransomware before encryption. But, you know, that is a call they have to make. We kind-of evaluate if they have cyber insurance or not and we kind-of walk them through those steps. But we try not to have them pay, but obviously some businesses do because if they don't they may not be back in business simply for the fact that they are going to be down for an extended period of time or they cannot restore their systems back to where they should be.

Chairwoman SLOTKIN. Right. But you certainly from the Michigan State Police perspective are not going to do anything punitive against an organization that decides to pay ransom, because you can understand no one likes that idea, we don't like to give money to bad guys and embolden them, but you can certainly understand from a small local government's perspective, a business perspective, if it is going to cost $40,000 to pay a ransom versus $400,000 to recover your data, you know, for your students who are a week from graduating, you can understand how these awful choices, you know, this devil's bargain that you have to make.

Mr. ELLIS. Absolutely. They oftentimes do pay just for those circumstances because that is—timing is what they weigh and often times, like you stated in your example, if they can be up and running in a short amount of time by paying the ransom, they will do that.

Chairwoman SLOTKIN. Great.

The Chair will now recognize other Members for questions they may wish to ask the witnesses.

The Chair recognizes for 5 minutes the gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you so very much. Again, let me emphasize the importance of the information this is being generated and should frankly be emphasized as we interact with local communities throughout the Nation.

So let me start. My questions will be to both the gentleman, Mr. Ellis, First Lieutenant, and the chief information officer, Ms. Clark.

I would be interested in—and I guess it is reaffirming some of the points that you made earlier about the current barriers that exist for small businesses and local communities in the way of sufficient cyber fortification and what role would educational initiatives and training play.

As you do that, let me ask, Madam Chair, to introduce into the record a time line of the biggest ransomware attacks dated—bitcoin

and other cryptocurrencies have been a key tool in on-line crime and I just, before the witnesses answer, mention Colonial Pipeline—these are large entities—paid $4.4 million, CNN financial paid $40 million. So we know that the big companies are paying dollars, we know that this is difficult for smaller entities.

[The information follows:]

A TIMELINE OF THE BIGGEST RANSOMWARE ATTACKS

Bitcoin and other cryptocurrencies have become a key tool in online crime.

CNET, Julian Dossett, Nov. 15, 2021 12:45 p.m. PT

The history of technology is riddled with unintended consequences. As William Gibson wrote in Burning Chrome, " . . . the street finds its own uses for things." Though Bitcoin may not have been originally conceived as a medium for ransom payments, it's quickly become a central tool for online criminals.

Ransomware, a category of "malware," blocks access to a computer or network until a ransom is paid. Despite the evolving efforts of governments to regulate cryptocurrency and mitigate its role in ransomware payments, the attacks keep coming.

Cryptocurrency ransomware payments totaled roughly $350 million in 2020, according to Chainanalysis—an annual increase of over 300 percent from 2019. And because U.S. companies are legally required to report cyberattacks only if customers' personal information is compromised, that estimate may be far too conservative.

Below, we tally up the damage of some of the highest-profile episodes.

Kaseya (2021)

On July 2, 2021, Kaseya announced its systems had been infiltrated. Kaseya provides IT solutions for other companies—an ideal target which, in a domino effect, ended up impacting approximately 1,500 organizations in multiple countries. REvil, a cybercriminal outfit, claimed responsibility for the attack and demanded ransoms ranging from a few thousand dollars to multiple millions, according to a Reuters report.

It's unclear how many individual businesses paid up, but REvil demanded $70 million in bitcoin from Kaseya. Kaseya declined to pay, opting to cooperate with the FBI and the U.S. Cybersecurity and Infrastructure Agency. On July 21, 2021, Kaseya obtained a universal decryptor key and distributed it to organizations impacted by the attack.

JBS (2021)

On May 31, 2021, JBS USA, one of the largest meat suppliers in the U.S., disclosed a hack that caused it to temporarily halt operations at its five largest U.S.-based plants. The ransomware attack also disrupted the company's Australia and UK operations. JBS paid the hackers an $11 million ransom in Bitcoin to prevent further disruption and limit the impact on grocery stores and restaurants. The FBI attributed the hack to REvil, a sophisticated criminal ring well-known in ransomware attacks.

Colonial Pipeline (2021)

On May 7, 2021, America's largest "refined products" pipeline went off-line after a hacking group called Darkside infiltrated it with ransomware. Colonial Pipeline covers over 5,500 miles and transports more than 100 million gallons of fuel daily. The impact of the attack was significant: In the days that followed, the average price of a gallon of gas in the U.S. increased to more than $3 for the first time in 7 years as drivers rushed to the pumps.

The pipeline operator said it paid the hackers $4.4 million in cryptocurrency. On June 7, 2021, the DOJ announced it had recovered part of the ransom. U.S. law enforcement officials were able to track the payment and take back $2.3 million using a private key for a cryptocurrency wallet.

Brenntag (2021)

On April 28, 2021, German chemical distributor Brenntag learned it was the target of a cyber attack by Darkside, which stole 150GB of data that it threatened to leak if ransom demands weren't met. After negotiating with the criminals, Brenntag ended up negotiating the original ransom of $7.5 million down to $4.4 million, which it paid on May 11.

CNA Financial (2021)

On March 23, 2021, CNA Financial, the seventh largest commercial insurer in the U.S., disclosed it had "sustained a sophisticated cybersecurity attack." The attack was carried out by a group called Phoenix, which used ransomware known as Phoenix Locker. CNA Financial eventually paid $40 million in May to get the data back. While CNA has been tight-lipped on the details of the negotiation and transaction, but says all of its systems have since been fully restored.

CWT (2020)

On July 31, 2020, U.S. business travel management firm CWT disclosed it had been impacted by a ransomware attack that infected its systems—and that it had paid the ransom. Using ransomware called Ragnar Locker, the assailants claimed to have stolen sensitive corporate files and knocked 30,000 company computers offline.

As a service provider to one-third of S&P 500 companies, the data release could have been disastrous for CWT's business. As such, the company paid the hackers about $4.5 million on July 28, a few days before Reuters reported the incident.

University of California at San Francisco (2020)

On June 3, 2020, the University of California at San Francisco disclosed that the UCSF School of Medicine's IT systems had been compromised by a hacking collective called Netwalker on June 1. The medical research institution had been working on a cure for COVID.

Apparently, Netwalker had researched UCFS, hoping to gain insights into its finances. Citing the billions of dollars UCFS reports in annual revenue, Netwalker demanded a $3 million ransom payment. After negotiations, UCSF paid Netwalker the bitcoin equivalent of $1,140,895 to resolve the cyberattack. According to the BBC, Netwalker was also identified as the culprit in at least two other 2020 ransomware attacks targeting universities.

Travelex (2019)

On New Year's Eve 2019, London-based foreign currency exchange Travelex was infiltrated by a ransomware group called Sodinokibi (aka REvil). The attackers made off with 5GB of customer data, including dates of birth, credit card information, and insurance details. Travelex took down its website in 30 countries in an attempt to contain the virus.

In the wake of the ransomware attack, Travelex struggled with customer services. Sodinokibi initially demanded a payment of $6 million (£4.6 million). After negotiations, Travelex paid the cybercriminals $2.3 million (285 BTC at the time, roughly £1.6 million) to get its data back.

WannaCry (2017)

In May 2017, a ransomware called WannaCry infected computers across the globe by exploiting a vulnerability in Windows PCs. The WannaCry vulnerability was revealed during a massive leak of NSA documents and hacking tools engineered by a group called Shadow Brokers in April 2017.

Though the exact number of WannaCry victims remains unknown, more than 200,000 computers around the world were infected. Victims included Spanish telecommunications company Telefonica and thousands of hospitals in the U.K. Computer systems in 150 countries were affected by the attack, with a total estimated loss of around $4 billion globally.

The attackers initially demanded $300 in bitcoin to unlock infected computer systems. The demand was later increased to $600 in bitcoin. However, some researchers claim that no one got their data back, even if they met the demands.

WannaCry attacks continue to this day. In February 2021, the DOJ indicted three North Korean computer programmers for their alleged role in the WannaCry outbreak.

Locky (2016)

Discovered in February 2016, Locky is notable due to the incredibly high number of infection attempts it's made on computer networks. Attacks typically come in the form of an email with an invoice attached from someone claiming to be a company employee. On February 16, 2016 analysis from Check Point identified more than 50,000 Locky attacks in 1 day.

Locky has many variants, but the goal is largely the same: Lock computer files to entice owners to pay a ransom in cryptocurrency in exchange for a decryption tool, which would allow users to regain access to their locked files. The majority of Locky victims have been in the U.S., and especially among health care companies, but Canada and France experienced significant infection rates as well.

TeslaCrypt (2015)

Modeled on an earlier program called CryptoLocker, the earliest TeslaCrypt samples were circulated in November 2014 but the ransomware was not widely distributed until March of the following year.

TeslaCrypt initially targeted gamers. After infecting a computer, a pop-up would direct a user to pay a $500 ransom in bitcoin for a decryption key to unlock the infected system. Other sources report the requested ransoms ranged from $250 to $1,000 in Bitcoin. In May 2016, the developers of Tesla Crypt released a master decryption key for affected users to unlock their computers.

CryptoWall (2014)

Widespread reports of computer systems infected from the CryptoWall ransomware emerged in 2014. Infected computers were unable to access files—unless the owner paid for access to a decryption program. Crypto Wall impacted systems across the globe. The attackers demanded payment in the form of prepaid cards or bitcoin. CryptoWall caused roughly $18 million in damages, according to Help Net Security. Multiple versions of CryptoWall were released, with each version making the ransomware more difficult to trace and combat.

CryptoLocker (2013)

The first time much of the world heard the term "ransomware" was during 2013's CcyptoLocker outbreak. Discovered early in September 2013, CryptoLocker would cripple more than 250,000 computer systems during the following 4 months. Victims were instructed to send payments in cryptocurrency or money cards to regain access. The ransomware delivered at least $3 million to its perpetrators.

A multinational law enforcement effort in 2014 succeeded in taking down the Gameover Zeus botnet, which was a primary distribution method for CryptoLocker. The DOJ indicted Russian hacker Evgeniy Mikhailovich Bogachev, as the botnet's ringleader. Bogachev is still at large—and the FBI is currently offering a reward of up to $3 million for information leading to his arrest and/ or conviction.

AIDS Trojan/PC Cyborg (1989)

Widely considered the template for all subsequent attacks, the AIDS Trojan (aka PC Cyborg) is the first known instance of a ransomware attack. In 1989, more than a decade before the creation of bitcoin, a biologist named Joseph Popp distributed 20,000 floppy disks at the World Health Organization AIDS conference in Stockholm. The floppy disks were labeled "AIDS Information—Introductory Diskettes" and contained a trojan virus that installed itself on MS–DOS systems.

Once the virus was on a computer, it counted the times the computer booted up. Once the computer booted up 90 times, the virus hid all directories and encrypted filenames. An image on the screen from the 'PC Cyborg Corporation' directed users to mail $189 to a P.O. address in Panama. The decryption process was relatively simple, however, and security researchers released a free tool to help victims.

Ms. JACKSON LEE. Would you be able to answer that question about the barriers that may exist?

Mr. ELLIS. Yes. Some of the barriers—thank you for the question—some of the barriers that do exist are, you know, lack of education and training, which we try to provide to many businesses, to be more cybersecurity-aware, thinking a little more along the lines of defensiveness when it comes to cybersecurity. Try to get them into security awareness training. We will go through best practices of which, you know, looking at defense-in-depth, looking at two-factor authentication, having a validated off-line back-up that they can restore data, have a remediation plan or continuity plan so they are able to get back up and running. Basically just looking at it from that point on as they move forward. You know, if this incident does occur or occurs again, what exactly will they do, who will they call, can their business survive, what best practices can they initiate being off-line? Just some of those things. We always look at best practices to try to get them back up and running again, but will also advise on potential resources that may get them back up and running.

Education and awareness is obviously paramount for some of the smaller and medium businesses in Michigan.

Ms. JACKSON LEE. Ms. Clark.

Chairwoman SLOTKIN. Sorry, ma'am, she is suffering from COVID and wasn't able to join us today.

Ms. JACKSON LEE. All right. Thank you. I am sorry, I thought I heard—let me then follow up with Mr. Ellis in particular about the work of MC3, including the Michigan Internet Crimes Against Children Task Force. That collaborates with Federal, State, and local partners to investigate offenders who use the internet on-line communication systems.

How does the ICAC Task Force work to educate children, parents, and schools on internet safety in the face of cyber predators?

Mr. ELLIS. Thank you for the question.

We educate parents, schools, our young adults in school by doing presentations, outreach. We will run through case scenarios with them so they understand, you know, what the potential is of them posting pictures on-line, which many kids do now, as you know. You know, sextortion is one of the big crimes or potential crimes that are going on, depending on how far it goes. That is affecting our young kids now. Again, a lot of it is education of our young people just to know that because they are so involved in social media, they are posting their lives on-line, what exactly that can mean to somebody that is potentially seeking them out as a potential victim.

Ms. JACKSON LEE. Can the Federal Government do more with respect to legislation to help you? Help that task force or help task forces across the country?

Mr. ELLIS. As far as legislation, you know, that is a great question. Anything that would allow for additional funding to allow for education. Maybe mandatory cybersecurity education in schools as part of the curriculum would be paramount so they get it at a young age. That would be—you know, that would also draw an interest in other areas, just so they can see and become acquainted with cybersecurity best practices.

Ms. JACKSON LEE. Thank you so very much.

I think my time has expired and——

Chairwoman SLOTKIN. Thank you, Congresswoman.

I would just say that there is a real interest on our committee on how to deal—I had never heard the term you mentioned for exploiting kids and sensitive pictures on-line. Can you repeat the term?

Mr. ELLIS. Sextortion.

Chairwoman SLOTKIN. Sextortion. I was not familiar with that term, but our committee has passed a bunch of legislation on K–12 resources and money basically for our K–12 schools to be able to learn and educate themselves and protect our kids' data, as well as digital literacy. Like how do we start teaching digital literacy to our kids at a very young age since they are the ones who are digital natives?

The Chair will now recognize for 5 minutes the gentlewoman from Florida, Mrs. Demings.

Mrs. DEMINGS. Well, thank you so much again, Chairwoman Slotkin, and thank you to Detective First Lieutenant Ellis for being

with us today. Thank you for your very impressive record of service with the Michigan State Police. As a former law enforcement officer, you know, we said 30 years ago that we could not fight today's battles with yesterday's weapons. My goodness, when we look at how the landscape has changed, that certainly rings true today. It is certainly not the same old Economic Crimes Unit or the Crimes Against Children Unit.

You know, so, Detective, I would love for you to just talk just a little bit about how policing has changed in this space, how the work force has had to change the level of training, the level of cooperation between you and other jurisdictions. You said that cyber crimes have no State-wide boundaries, and boy is that true. But how has the level of cooperation changed or what challenges have occurred because of those no State-wide boundaries that you face?

Mr. ELLIS. Thank you for the question.

Yes, we have seen within Michigan the fact that we are the Michigan State Police and we act as resource for those other 580 law enforcement agencies in Michigan and others around the Nation, we see a lack of trained officers in the realm of the recovery of digital evidence, or even what devices may contain digital evidence that may be a part of a crime. You know, everybody typically knows a mobile device or their phone contains a lot of evidence or someone's patterns of life, but with some of the other devices, that it comes to our automobiles, obviously our computer systems, smart TVs, personal assistant devices. If you think of all the things we interact with that could be a potential part of a crime, those officers need to be trained when they are responding to an incident what potentially could contain evidence.

So we are trying to educate them the best we can through a lot of education opportunities. When have our recruit schools for new troopers we have a segment training them on scenarios. So the biggest thing we can do is continue our training and education. We bring local officers into our office as pseudo full-time members working as affiliates to investigate digital crime. Once their department sees how valuable they are and an asset to their agency, it is good for us because we can keep them and the police organizations typically want them involved to get training.

There is a lot of industry standard training that can be taken just regarding evidence recovery and knowing cybersecurity in general—if I can put it that way. But a lot of our younger people are more apt to the devices and the capabilities because they grew up with it in their hands. So some of our younger folks are easily more trained than maybe some of us were a few years ago.

Mrs. DEMINGS. Of course that is not just a challenge for Michigan. You know, in Florida, and really across the Nation, really making sure that your work force keeps up with the challenges and the technology of the day.

How would you say the Federal Government could assist in this area more? Is that through CISA making resources more available for training opportunities?

Mr. ELLIS. Thank you for the question.

We are always up for additional training and assistance. DHS CISA is an excellent partner in Michigan of ours. We collaborate on a lot of different initiatives and take advantage of training. It

is like I tell all my folks in the Michigan Cyber Command Center, the more training, the better, along with our affiliates, and even our analysts that are on board. In these days the general officer on the road should be taking some type of cybersecurity-related training to help them with their investigations, without a doubt.

Mrs. DEMINGS. Well, again, thank you so much for your service. We are working on some legislation that involves the digital technology area, including training for law enforcement officers. So I am hoping that we will be able to move that through very, very quickly.

Thank you.

Madam Chair, I yield back.

Chairwoman SLOTKIN. Thank you. Those sounded like good questions from a former police chief of a major city. That sounded about right.

So let me just ask for the Michiganders in the room and watching, help us understand what an average ransomware attack looks like in the State of Michigan. Maybe go through—you can pick one that is representative of a closed investigation. You don't have to give any identifiable information. But walk us through what that looks like.

Then same thing on sexploitation. You have a whole unit that is worried about this. Help us understand in detail what those cases look like so parents and business owners understand what they are looking for.

Mr. ELLIS. Sure. Typically in a ransomware event—and I can, you know, look as far back as yesterday morning. This is not really any different than any other ransomware case that is local to a business in Michigan. They will notice that their files are encrypted. As most users, once files are encrypted it is obvious because you can't access your files. They get messages on the screens, wallpapers change on your desktop, that kind of thing.

They will call, we will go through an evaluation with them. We typically bring on more partners sometimes, depending on the business. We often times will include our Federal partners in the discussion just to walk through the steps and look at where they are at, are they able to recover. Oftentimes they may have cyber insurance and that initially limits us from getting potential evidence, at least initially, depending if legal is involved. But otherwise our first avenue is to try to obtain evidence and, you know, if their IT staff or if we can get an image of a device to try and locate those indicators of compromise, we will do that and help them understand what happened on their network and, like I said earlier, take that information back to push it back out to everybody else for prevention and awareness.

Oftentimes they will look for resources for those small-to-medium businesses that don't have a plan, aren't sure what to do. We will help guide them in that respect. Within Michigan we also have the Michigan Cyber Civilian Corps. If they have several work stations that they need assistance with or they are not sure how maybe the incident happened or need, you know, hands on keyboards, the Michigan Cyber Civilian Corps, or MiC3, is a group of volunteers that have been vetted that work in Michigan businesses——

Chairwoman SLOTKIN. You all would connect them to the——

Mr. ELLIS. We would connect them, they become indemnified as State employees and they can assist with the recovery of an incident.

Chairwoman SLOTKIN. This incident that you were investigating yesterday morning, what are they asking for, how much money? Like give us a little bit of a flavor of the threat.

Mr. ELLIS. Yes, in this case, you know, I can tell you end-point-wise they have 100 end-points——

Chairwoman SLOTKIN. What is an end-point?

Mr. ELLIS. A device that a user sits at. A keyboard that somebody uses. They may have—I don't know that they announced their ransom yet because we went to that site—they are getting creative where they will tell you they will provide you a link to go to and this site was down all day yesterday. So lack of planning on their end to be able to obtain their ransom. But typically, depending on the small-to-medium business, it can be anywhere from $20,000 to $100,000 depending on what is at stake. Typically the bad actors know what data they have, what they have access to obviously, and, you know, the prime data goes for a bigger price.

Chairwoman SLOTKIN. Is it fair to say that some of these organizations, these bad actors, have done research, they have looked on social media, they have looked on public transparency websites? Like they have done their homework on an organization before they decide to ransom them?

Mr. ELLIS. Absolutely. They know price points, they know the budget, they know if a school is being remodeled over the summer based on the RFP, who won the bid. I mean they are going in there with knowledge and have chosen a target that they think they can succeed at.

Chairwoman SLOTKIN. Then, again, explain the threat, or just a recent example on the sexploitation. Sort-of how do they use children's data or how do they ransom it or use it to make money?

Mr. ELLIS. Yes. Sextortion is typically pictures are taken or relationships are built through chat on same old device or Snapchat or any other messaging platform. They will gain the user's confidence—usually this is big with students right now, younger people—and get them to send a provocative picture. Oftentimes they are misrepresenting themselves as maybe—if they are chatting with a male they may represent themselves as a young female, attractive, sending pictures—normal pictures, not anything provocative—and eliciting pictures back. Once they finally do send a picture back, they will then demand that they pay a ransom or a payment, otherwise they will publish the photo publicly. As you can imagine, being at that age, when your identity is everything, social media is everything, that is, you know, not something you would want among your peers.

Just recently we have had a case where this happened and our young gentleman paid the fee that was being asked. The person had indicated prior they would remove any pictures that they had possession of, but then again came back and asked for more. Unfortunately this student committed suicide over this. This all occurred within a 6-hour period in Michigan.

Chairwoman SLOTKIN. Oh.

Mr. ELLIS. So it has devastating effects and it is one of the fastest-growing incidents that we are seeing among young people right now.

Chairwoman SLOTKIN. Oh, gosh. OK. Well, I have much more to ask about that. But we are on to a second round of questions.

Ready for recognition? Oh, OK. Sorry, I was supposed to recognize myself.

So let me just ask, can a young person under 18—is there any rules around whether they are able to pay? I mean did this young person handle it themselves? What are the protections for people under 18 that are maybe different from an adult?

Mr. ELLIS. They can handle it themselves. In this case, and several cases, they do because they do not want anybody to know.

Typically in these type of cases, the people, younger people, our kids, don't want anything to know about—they don't want their parents to know about it or their relatives or their friends. So those that typically should be closest to them, they are most embarrassed over. We are finding that—as far as age, you know, we do have some that go to their parents and request payment and that starts another whole investigation.

I will say on the investigation that I did just mention, thanks to our Federal partners, we have located somebody that we are confident we will be able to take action against.

Chairwoman SLOTKIN. Great. So are the folks who are ransoming our young people for, you know, these explicit pictures, do they have a different threat profile than some of the ransomware folks? Is it still folks who are coming from overseas or is it much more local? Kind-of what is the intent other than to ransom folks? Are they then going on and using it, you know, for pornography online? Just like help us understand what might be different from—you know, are they more local basically?

Mr. ELLIS. Yes. The majority of cases we see they are not local. The person I am referring to that is a suspect was in Nigeria.

Chairwoman SLOTKIN. Oh.

Mr. ELLIS. So they are looking at kids, they are looking at social media pages. I mean they are portraying a friend that gets accepted into their friend community and learn everything they can about them, establish a relationship, and, you know, the student has no idea who they are talking to. So it is very unfortunate.

But, yes, the motivation is a little bit different. They know they are not going to get a lot of money out of a younger person and, you know, compared to a ransomware where they may hit a business that has deeper pockets potentially. But again they can go after several students, gain these relationships over time. A lot of the suspects we are seeing are younger, so we are still in the research phase of are they going to be moving on to bigger and better things, are they a quick-hit opportunity to get a few hundred dollars, or a little bit more.

So, yes, there is a lot of research going on into that right now.

Chairwoman SLOTKIN. So, again, just to give people a sense of the threat, this young person who was ransomed and then ended up, you know, terribly committing suicide over the potential exposure, how much money are we talking about? What was the request for ransom?

Mr. ELLIS. Less than $1,000.

Chairwoman SLOTKIN. Then just for the young people, if you have got a 16- or a 17-year-old, who of course is deeply embarrassed in front of their community to admit that they sent these photos, if they contact law enforcement will their parents be contacted?

Mr. ELLIS. Depending on the circumstance and their age—depending. I will say the circumstances can be different. Typically we will notify a parent. Obviously if they are over 17, that doesn't always happen just because of their age in Michigan and legal requirements. But, yes, I mean we will notify a parent, a trusted guardian, or if they have a relative we can start there. But typically we will talk them into why they need to contact a parent or let them know that, you know, it is going to be OK and why we need to contact their parent.

Chairwoman SLOTKIN. Yes.

Mr. ELLIS. Just because of the potential outcome.

Chairwoman SLOTKIN. I think the thing that ties the issue of sexploitation and just ransomware in general for businesses and local officials is how these bad actors pull threads from publicly-available information, right. As a former CIA officer and Pentagon official, we are taught—just it is—we are beaten over the head on you shouldn't put out personally identifiable information, talk about where you are going on vacation, talking about that new deck that you are building on that house. That kind of stuff can be pieced together so that people can basically breed familiarity so that they—it seems like they know you really well, they are someone who is in your kind-of community or that just they have figured out you are spending money on things, the things that you value in your life and what you would be willing to pay to protect.

So, you know, for folks who are not in law enforcement or come from an intelligence background, talk about personally identifiable information. Particularly we talked in the last session about how that helps people figure out passwords and answers to security questions. Just talk about how those bad actors piece the stories together.

Mr. ELLIS. Sure. I mean if you think about—good question, and thank you.

If you think about the average social media account, depending how active anyone in this room may be, there are some people that are very active and they post everything from pictures of their home, their vehicles, what they eat—I mean you name it, every activity of their day is on-line. Oftentimes you can build a tremendous profile and get to know a pattern of life of somebody from their address, based on photos, where they are going to be playing ball that night, where dance practice is going to be. They think they are just taking pictures of their friends, but if you start looking in the background you can piece all this together.

So it is very important to parents to know what their children are doing, know what their young adults are doing. Pay attention, ask questions, look on their accounts. They will be glad you did in the long run. You can kind-of see if you can put a pattern of life together based on what they are posting.

Chairwoman SLOTKIN. Thank you for that.

The Chair now recognizes for 5 minutes the gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you, again, Madam Chair, for this hearing. I want to express my appreciation for the witnesses on the first panel from the Department of Homeland Security and I hope it exposed to the Nation, to the great resources that we have in the Federal Government, and also the work, legislative work that has been done by this committee, by the full committee and Chairman Thompson, and the work that I have done regarding zero-day incidences in trying to ensure that major attacks against much of our infrastructure does not bring America to a point of disaster.

Working with local communities is certainly an important moment and it is an important moment because it provides education.

So I would be interested, and if said before I ask you to say it again, as I have taken note of the attacks from the medical center in Yuma, Arizona in April, Texas Tech in my State announced that the ECL ransomware attack in December potentially affected 1.29 million of their patients. This can be a deep dive into the personal lives of individuals and private information.

So I would be interested, again, if you would State if you put in policies that provide a wall of infrastructure around potential cyber ransomware attacks.

Also should we—I think I heard a discussion about insurance—should there be a mechanism to compensate those who have been harmed—this is a crime, but it is also in the civil sphere as well—by the loss of their data? I think it is really something that is a new phenomenon. Children are hurt, families are hurt, patients are hurt, small businesses are hurt. I think we need to emphasize this as a larger question than sometimes what it may be predicted.

So with your years of law enforcement experience, I am sure you have had to solve cases, you have seen crime victims, what would be your viewpoint on how we address the elements that I have said, the loss of data, the impact on an individual or business, and the kind of infrastructure we should stand up to be much safer.

Lieutenant Ellis.

Mr. ELLIS. Thank you for the question.

You know, it comes down to security and it is—your question would actually solve a lot of things if we knew what that answer was as far as infrastructure. Because one of the things we face, even with those in cybersecurity that are putting all the protections in place with firewalls, IDS, IPS, all the security devices, user awareness training, there is always something new coming out based on new software, new technologies. I feel like we would always be chasing down new solutions.

There are solutions out there that will protect data itself versus the infrastructure that the data resides on or traverses. They are expensive solutions, they are typically at the Federal level and just coming into play now. We are hoping to see more of this. Essentially what that is is—I have just seen samples of this where you can pretty much put any kind of data in the worst environment and it really cannot be used in any way, even if they exfiltrated it. It is impervious to malware. There are solutions out there. They are expensive. You know, that is one solution when some people

find out or entities and businesses find out about this, the common question is why doesn't everybody use these solutions?

It typically comes down to price, unfortunately. But that is just one way that you could help combat this. But I feel like there is no one solution that is going to solve all of this immediately with how we do things today when it comes to cyber.

Ms. JACKSON LEE. Let me thank you so very much.

Madam Chair, as I yield back let me thank you for this hearing that has been enormously informative. I think Mr. Ellis has left us with next steps in particularly how we can assist States across America. Focusing on Michigan and the local needs and the local insights I think has been vital for this full committee.

I look forward to working with you back in Washington to be sure we take this very vital information and incorporate it into solutions to some of the issues being raised here by these representatives from your State and of course those from the Department of Homeland Security.

Thank you so very much. Again, thank you for your leadership and I am yielding back.

Thank you.

Chairwoman SLOTKIN. Thank you, Congresswoman.

With that, I thank the witness for his valuable time and testimony and the Members for their questions. Thanks for the opportunity to just pulse you one-on-one on how our Michigan organizations can protect themselves.

I urge again all of our businesses, our farmers, our K–12 schools, our local electeds to get to know Mr. Ellis and his team before you have a problem. Take all your friends in the sector that you come from, ask for a meeting.

I know that him and his team are very responsive and you can understand how to protect yourself. Have a relationship, have a business card before you have a major incident, since we know that chances are folks in the room are going to be on the wrong end of a ransomware attack at some point in their careers unfortunately.

Members of the subcommittee may have additional questions for all of our witnesses. We ask that you respond expeditiously in writing to those questions. The Chair reminds Members of the subcommittee that the record will remain open for 10 business days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 12:54 p.m., the subcommittee was adjourned.]

○